entropy

MDPI

Article

Polar Coding for Confidential Broadcasting

Jaume del Olmo Alòs * and Javier Rodríguez Fonollosa

Departament de Teoria del Senyal i Communications, Universitat Politècnica de Catalunya, 08034 Barcelona, Spain; javier.fonollosa@upc.edu

* Correspondence: jaume.del.olmo@upc.edu

Received: 7 January 2020; Accepted: 24 January 2020; Published: 27 January 2020

Abstract: A polar coding scheme is proposed for the Wiretap Broadcast Channel with two legitimate receivers and one eavesdropper. We consider a model in which the transmitter wishes to send the same private (non-confidential) message and the same confidential message reliably to two different legitimate receivers, and the confidential message must also be (strongly) secured from the eavesdropper. The coding scheme aims to use the optimal rate of randomness and does not make any assumption regarding the symmetry or degradedness of the channel. This paper extends previous work on polar codes for the wiretap channel by proposing a new chaining construction that allows to reliably and securely send the same confidential message to two different receivers. This construction introduces new dependencies between the random variables involved in the coding scheme that need to be considered in the secrecy analysis.

Keywords: polar codes; information-theoretic security; wiretap broadcast channel; strong secrecy

1. Introduction

Information-theoretic security over noisy channels was introduced by Wyner in [1], which characterized the secrecy-capacity of the degraded wiretap channel. Later, Csiszár and Körner in [2] generalized Wyner's results to the general wiretap channel. In these settings, one transmitter wishes to reliably send one message to a legitimate receiver, while keeping it secret from an eavesdropper, where secrecy is defined based on a condition of some information-theoretic measure that is fully quantifiable. One of these measures is the *information leakage*, defined as the mutual information $I(W;Z^n)$ between a uniformly distributed random message W and the channel observations Z^n at the eavesdropper, n being the number of uses of the channel. Based on this measure, the most common secrecy conditions required to be satisfied by channel codes are the *weak secrecy*, which requires $\lim_{n\to\infty} \frac{1}{n} I(W;Z^n) = 0$, and the *strong secrecy*, requiring $\lim_{n\to\infty} I(W;Z^n) = 0$. Although the second notion of security is stronger, surprisingly both conditions result in the same secrecy-capacity [3].

In the last decade, information-theoretic security has been extended to a large variety of contexts, and polar codes have become increasingly popular in this area, due to their easily provable secrecy capacity achieving property. Polar codes were originally proposed by Arikan in [4] to achieve the capacity of binary-input, symmetric, and point-to-point channels under Successive Cancellation (SC) decoding. Secrecy capacity achieving polar codes for the binary symmetric degraded wiretap channel were introduced in [5] and [6], satisfying the weak and the strong secrecy condition, respectively. Recently, polar coding has been extended to the general wiretap channel in [7–10] and to different multiuser scenarios (for instance, see [11] and [12]). Indeed, [9] and [10] generalize their results providing polar codes for the broadcast channel with confidential messages.

This paper provides a polar coding scheme that allows to transmit *strongly* confidential common information to two legitimate receivers over the Wiretap Broadcast Channel (WTBC). Although [13] provided an obvious lower-bound on the secrecy-capacity of this model, no constructive polar coding scheme has already been proposed so far. Our polar coding scheme is based mainly on the one

introduced by [10] for the broadcast channel with confidential messages. Therefore, the proposed polar coding scheme aims to use the optimal amount of randomness in the encoding. Moreover, in order to construct an explicit polar coding scheme that provides strong secrecy, the distribution induced by the encoder must be close in terms of the statistical distance to the original one considered for the code construction, and transmitter and legitimate receivers need to share a secret key of negligible size in terms of rate. Nevertheless, the particularization for the model proposed in this paper is not straightforward. Specifically, we propose a new chaining construction [14] (transmission will take place over several blocks) that is crucial to secretly transmit common information to different legitimate receivers. Indeed, this model generalizes, in part, the one described in [10], where the confidential message is intended only for one legitimate receiver, and the one in [15], which considers only the transmission of non-confidential messages intended for two different receivers. The proposed chaining introduces new bidirectional dependencies between encoding random variables of adjacent blocks that must be considered carefully in the secrecy analysis. Indeed, we need to make use of an additional secret key of negligible size in terms of rate that is privately shared between transmitter and legitimate receivers, which will be used to prove that dependencies between blocks can be broken and, therefore, the strong secrecy condition will be satisfied.

1.1. Notation

Throughout this paper, let $[n] = \{1, \dots, n\}$ for $n \in \mathbb{Z}^+$, a^n denotes a row vector $(a(1), \dots, a(n))$. We write $a^{1:j}$ for $j \in [n]$ to denote the subvector $(a(1), \dots, a(j))$. Let $\mathcal{A} \subset [n]$, then we write $a[\mathcal{A}]$ to denote the sequence $\{a(j)\}_{j\in\mathcal{A}}$, and we use $\mathcal{A}^{\mathrm{C}}$ to denote the set complement with respect to the universal set $[n]$, that is, $\mathcal{A}^{\mathrm{C}} = [n] \setminus \mathcal{A}$. If $\mathcal{A}$ denotes an event, then $\mathcal{A}^{\mathrm{C}}$ also denotes its complement. We use ln to denote the natural logarithm, whereas log denotes the logarithm base 2. Let X be a random variable taking values in $\mathcal{X}$, and let q_x and p_x be two different distributions with support $\mathcal{X}$, then $\mathbb{D}(q_x, p_x)$ and $\mathbb{V}(q_x, p_x)$ denote the Kullback–Leibler divergence and the total variation distance respectively. Finally, $h_2(p)$ denotes the binary entropy function, i.e., $h_2(p) = -p \log p - (1-p) \log(1-p)$.

1.2. Organization

The remainder of this paper is organized as follows. Section 2 introduces the channel model formally. In Section 3, the fundamental theorems of polar codes are revisited. Section 4 describes the proposed polar coding scheme, and Section 5 proves that this polar coding scheme achieves the best known inner-bound on the secrecy-capacity of this model. Finally, the concluding remarks are presented in Section 6.

2. Channel Model and Achievable Region

Formally, a WTBC $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ with 2 legitimate receivers and an external eavesdropper is characterized by the probability transition function $p_{Y_{(1)}Y_{(2)}Z|X}$, where $X \in \mathcal{X}$ denotes the channel input, $Y_{(k)} \in \mathcal{Y}_{(k)}$ denotes the channel output corresponding to the legitimate Receiver $k \in [1,2]$, and $Z \in \mathcal{Z}$ denotes the channel output corresponding to the eavesdropper. We consider a model, namely Common Information over the Wiretap Broadcast Channel (CI-WTBC), in which the transmitter wishes to send a private message W and a confidential message S to both legitimate receivers. A code $\left(\lceil 2^{nR_W} \rceil, \lceil 2^{nR_S} \rceil, \lceil 2^{nR_R} \rceil, n\right)$ for the CI-WTBC consists of a private message set $\mathcal{W} \triangleq \left[1, \lceil 2^{nR_W} \rceil\right]$, a confidential message set $\mathcal{S} \triangleq \left[1, \lceil 2^{nR_S} \rceil\right]$, a randomization sequence set $\mathcal{R} \triangleq \left[1, \lceil 2^{nR_R} \rceil\right]$ (needed to confuse the eavesdropper about the confidential message S), an encoding function $f : \mathcal{W} \times \mathcal{S} \times \mathcal{R} \to \mathcal{X}^n$ that maps (w, s, r) to a codeword x^n, and two decoding functions $g_{(1)}$ and $g_{(2)}$ such that $g_{(k)} : \mathcal{Y}_{(k)}^n \to \mathcal{W} \times \mathcal{S}$ ($k \in [1,2]$) maps the k-th legitimate receiver observations $y_{(k)}^n$

to the estimates $(\hat{w}^{(k)}, \hat{s}^{(k)})$. The reliability condition to be satisfied by this code is measured in terms of the average probability of error and is given by

$$\lim_{n\to\infty} \mathbb{P}\left[(W,S) \neq (\hat{W}^{(k)}, \hat{S}^{(k)})\right] = 0, \quad k \in [1,2]. \tag{1}$$

The *strong* secrecy condition is measured in terms of the information leakage and is given by

$$\lim_{n\to\infty} I\left(S; Z^n\right) = 0. \tag{2}$$

This model is graphically illustrated in Figure 1. A triple of rates $(R_W, R_S, R_R) \in \mathbb{R}_+^3$ will be achievable for the CI-WTBC if there exists a sequence of $(\lceil 2^{nR_W} \rceil, \lceil 2^{nR_S} \rceil, \lceil 2^{nR_R} \rceil, n)$ codes such that satisfy the reliability and secrecy conditions (1) and (2), respectively.

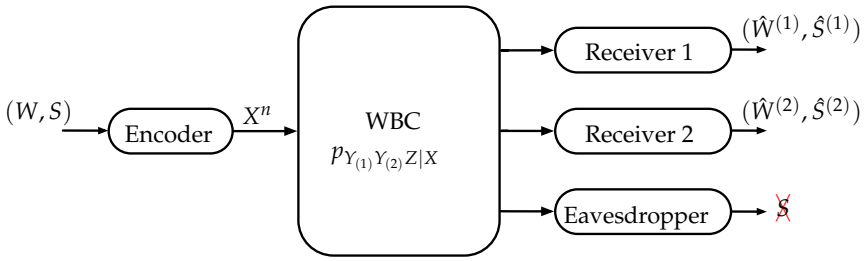

Figure 1. Channel model: CI-WTBC.

The achievable rate region is defined as the closure of the set of all achievable rate triples (R_W, R_S, R_R). The following proposition defines an inner-bound on this region.

Proposition 1 (Adapted from [13,16]). *The region* $\mathfrak{R}_{\text{CI-WTBC}}$ *defined by the union over the triples of rates* $(R_W, R_S, R_R) \in \mathbb{R}_+^3$ *satisfying*

$$\begin{aligned} R_W + R_S &\leq \min\left\{I(V;Y_{(1)}), I(V;Y_{(2)})\right\}, \\ R_S &\leq \min\left\{I(V;Y_{(1)}), I(V;Y_{(2)})\right\} - I(V;Z), \\ R_W + R_R &\geq I(X;Z), \\ R_R &\geq I(X;Z|V), \end{aligned}$$

where the union is taken over all distributions p_{VX} *such that* $V - X - (Y_{(1)}, Y_{(2)}, Z)$ *forms a Markov chain, defines an inner-bound on the achievable region of the CI-WTBC.*

In this model, the private message W introduces part of the randomness required to confuse the eavesdropper about the confidential message S, and the randomization sequence R denotes the additional randomness that is required for channel prefixing.

3. Review of Polar Codes

Let $(\mathcal{X} \times \mathcal{Y}, p_{XY})$ be a Discrete Memoryless Source (DMS), where $X \in \{0,1\}$ (Throughout this paper, we assume binary polarization. Nevertheless, an extension to q-ary alphabets is possible [10,17,18]) and $Y \in \mathcal{Y}$. The polar transform over the n-sequence X^n, n being any power of 2, is defined as $U^n \triangleq X^n G_n$, where $G_n \triangleq \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]^{\otimes n}$ is the source polarization matrix [19]. Since $G_n = G_n^{-1}$, then $X^n = U^n G_n$.

The polarization theorem for source coding with side information [19] (Th. 1) states that the polar transform extracts the randomness of X^n in the sense that, as $n \to \infty$, the set of indices $j \in [n]$ can be divided practically into two disjoint sets, namely $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$, such that $U(j)$ for $j \in \mathcal{H}_{X|Y}^{(n)}$ is

practically independent of $(U^{1:j-1}, Y^n)$ and uniformly distributed, i.e., $H(U(j)|U^{1:j-1}, Y^n) \to 1$, and $U(j)$ for $j \in \mathcal{L}_{X|Y}^{(n)}$ is almost determined by $(U^{1:j-1}, Y^n)$, i.e., $H(U(j)|U^{1:j-1}, Y^n) \to 0$. Formally, let

$$\mathcal{H}_{X|Y}^{(n)} \triangleq \{j \in [n] : H(U(j)|U^{1:j-1}, Y^n) \geq 1 - \delta_n\},$$
$$\mathcal{L}_{X|Y}^{(n)} \triangleq \{j \in [n] : H(U(j)|U^{1:j-1}, Y^n) \leq \delta_n\},$$

where $\delta_n \triangleq 2^{-n^\beta}$ for some $\beta \in (0, \frac{1}{2})$. Then, by Lemma 4 of [10] we have $\lim_{n\to\infty} \frac{1}{n}|\mathcal{H}_{X|Y}^{(n)}| = H(X|Y)$ and $\lim_{n\to\infty} \frac{1}{n}|\mathcal{L}_{X|Y}^{(n)}| = 1 - H(X|Y)$, which imply that $\lim_{n\to\infty} \frac{1}{n}|(\mathcal{H}_{X|Y}^{(n)})^{\mathrm{C}} \setminus \mathcal{L}_{X|Y}^{(n)}| = 0$, i.e., the number of elements that *have not been polarized* is asymptotically negligible in terms of rate. Furthermore, Th. 2 of [19] states that given $U[(\mathcal{L}_{X|Y}^{(n)})^{\mathrm{C}}]$ and Y^n, $U[\mathcal{L}_{X|Y}^{(n)}]$ can be reconstructed using SC decoding with error probability in $O(n\delta_n)$. Alternatively, the previous sets can be defined based on the Bhattacharyya parameters $\{Z(U(j)|U^{1:j-1}, Y^n)\}_{j=1}^n$ because both parameters *polarize* simultaneously Proposition 2 of [19]. It is worth mentioning that both the entropy terms and the Bhattacharyya parameters required to define these sets can be obtained deterministically from p_{XY} and the algebraic properties of G_n [20–22].

Similarly to $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$, the sets $\mathcal{H}_X^{(n)}$ and $\mathcal{L}_X^{(n)}$ can be defined by considering that observations Y^n are absent. A discrete memoryless channel $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ with some arbitrary p_X can be seen as a DMS $(\mathcal{X} \times \mathcal{Y}, p_X p_{Y|X})$. In channel polar coding, first we define $\mathcal{H}_{X|Y}^{(n)}$, $\mathcal{L}_{X|Y}^{(n)}$, $\mathcal{H}_X^{(n)}$ and $\mathcal{L}_X^{(n)}$ from the target distribution $p_X p_{Y|X}$ (*polar construction*). Then, based on the previous sets, the encoder somehow constructs (since the polar-based encoder will construct random variables that must approach the target distribution of the DMS, throughout this paper we use *tilde* above the random variables to emphazise this purpose) $\tilde{U}^n$ and applies the inverse polar transform $\tilde{X}^n = \tilde{U}^n G_n$ with distribution $\tilde{q}_{X^n}$. Afterwards, the transmitter sends $\tilde{X}^n$ over the channel, which induces $\tilde{Y}^n \sim \tilde{q}_{Y^n}$. If $\mathbb{V}(\tilde{q}_{X^n Y^n}, p_{X^n Y^n}) \to 0$, then the receiver can reliably reconstruct $\tilde{U}[\mathcal{L}_{X|Y}^{(n)}]$ from $\tilde{Y}^n$ and $\tilde{U}[(\mathcal{L}_{X|Y}^{(n)})^{\mathrm{C}}]$ by using SC decoding [23].

4. Polar Coding Scheme

Let $(\mathcal{V} \times \mathcal{X} \times \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z}, p_{VXY_{(1)}Y_{(2)}Z})$ denote the DMS that represents the input (V, X) and output $(Y_{(1)}, Y_{(2)}, Z)$ random variables of the CI-WTBC, where $|\mathcal{V}| = |\mathcal{X}| \triangleq 2$. Without loss of generality, and to avoid the trivial case $R_S = 0$ in Proposition 1, we assume that

$$H(V|Z) > H(V|Y_{(1)}) \geq H(V|Y_{(2)}). \tag{3}$$

If $H(V|Y_{(1)}) < H(V|Y_{(2)})$, one can simply exchange the role of $Y_{(1)}$ and $Y_{(2)}$ in the polar coding scheme described in Section 4. We propose a polar coding scheme that achieves the following rate triple,

$$(R_W, R_S, R_R) = (I(V;Z), I(V;Y_{(1)}) - I(V;Z), I(X;Z|V)), \tag{4}$$

which corresponds to the one of the region in Proposition 1 such that the private and the confidential message rate are maximum and the amount of randomness is minimum.

For the input random variable V, we define the polar transform $A^n \triangleq V^n G_n$ and the sets

$$\mathcal{H}_V^{(n)} \triangleq \{j \in [1,n] : H(A(j)|A^{1:j-1}) \geq 1 - \delta_n\}, \tag{5}$$
$$\mathcal{H}_{V|Z}^{(n)} \triangleq \{j \in [1,n] : H(A(j)|A^{1:j-1}Z^n) \geq 1 - \delta_n\}, \tag{6}$$
$$\mathcal{L}_{V|Y_{(k)}}^{(n)} \triangleq \{j \in [1,n] : H(A(j)|A^{1:j-1}Y_{(k)}^n) \leq \delta_n\}, \quad k = 1,2. \tag{7}$$

For the input random variable X, we define $T^n \triangleq X^n G_n$ and the associated sets

$$\mathcal{H}_{X|V}^{(n)} \triangleq \{j \in [1,n] : H(T(j)|T^{1:j-1}V^n) \geq 1-\delta_n\}. \tag{8}$$

$$\mathcal{H}_{X|VZ}^{(n)} \triangleq \{j \in [1,n] : H(T(j)|T^{1:j-1}V^nZ^n) \geq 1-\delta_n\}. \tag{9}$$

We have $p_{A^nT^n}(a^n,t^n) = p_{V^nX^n}(a^nG_n, t^nG_n)$, due to the invertibility of G_n, and we write

$$p_{A^nT^n}(a^n,t^n) = \left(\prod_{j=1}^{n} p_{A(j)|A^{1:j-1}}(a(j)|a^{1:j-1})\right)\left(\prod_{j=1}^{n} p_{T(j)|T^{1:j-1}V^n}(t(j)|t^{1:j-1}, a^nG_n)\right).$$

Consider that the encoding takes place over L blocks indexed by $i \in [1,L]$. At the i-th block, the encoder will construct $\tilde{A}_i^n$, which will carry the private and the confidential messages intended for both legitimate receivers. Additionally, the encoder will store into $\tilde{A}_i^n$ some elements from $\tilde{A}_{i-1}^n$ (if $i \in [2,L]$) and $\tilde{A}_{i+1}^n$ (if $i \in [1,L-1]$), so that both legitimate receivers are able to reliably reconstruct $\tilde{A}_{1:L}^n$. Then, given $\tilde{V}_i^n = \tilde{A}_i^n G_n$, the encoder will perform the polar-based channel prefixing to construct $\tilde{T}_i^n$. Finally, it will obtain $\tilde{X}_i^n = \tilde{T}_i^n G_n$, which will be transmitted over the WTBC, inducing the channel output observations $(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$.

Consider the construction of $\tilde{A}_{1:L}^n$. Besides, sets in (5)–(7), define the partition of $\mathcal{H}_V^{(n)}$:

$$\mathcal{G}^{(n)} \triangleq \mathcal{H}_{V|Z}^{(n)}, \tag{10}$$

$$\mathcal{C}^{(n)} \triangleq \mathcal{H}_V^{(n)} \cap (\mathcal{H}_{V|Z}^{(n)})^{\mathrm{C}}. \tag{11}$$

Moreover, we also define the following partition of the set $\mathcal{G}^{(n)}$:

$$\mathcal{G}_0^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{12}$$

$$\mathcal{G}_1^{(n)} \triangleq \mathcal{G}^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{13}$$

$$\mathcal{G}_2^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}, \tag{14}$$

$$\mathcal{G}_{1,2}^{(n)} \triangleq \mathcal{G}^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}, \tag{15}$$

and the following partition of the set $\mathcal{C}^{(n)}$:

$$\mathcal{C}_0^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{16}$$

$$\mathcal{C}_1^{(n)} \triangleq \mathcal{C}^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{17}$$

$$\mathcal{C}_2^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}, \tag{18}$$

$$\mathcal{C}_{1,2}^{(n)} \triangleq \mathcal{C}^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}; \tag{19}$$

These sets are graphically represented in Figure 2. Roughly speaking, $A[\mathcal{H}_V^{(n)}]$ is the *nearly uniformly* distributed part of A^n. Thus, $\tilde{A}_i[\mathcal{H}_V^{(n)}]$, $i \in [1,L]$, is suitable for storing uniformly distributed random sequences. The sequence $A[\mathcal{H}_{V|Z}^{(n)}]$ is *almost* independent of Z^n and, hence, $\tilde{A}_i[\mathcal{G}^{(n)}]$ is suitable for storing information to be secured from the eavesdropper, whereas $\tilde{A}_i[\mathcal{C}^{(n)}]$ is not. Sets in (12)–(19) with subscript 1 (sets inside the red curve in Figure 2) form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}$, while those with subscript 2 (sets inside the blue curve) form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}$. From Th. 2 of [19] and [23], recall

that $\tilde{A}_i[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(k)}}^{(n)})^{\mathrm{C}}]$ is the nearly uniformly distributed part of the sequence $\tilde{A}_i^n$ required by legitimate Receiver k to reliably reconstruct the entire sequence by performing SC decoding.

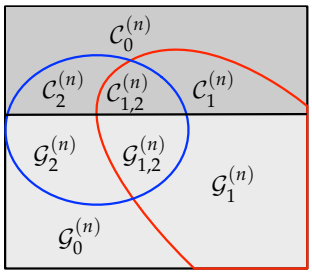

Figure 2. Graphical representation of the sets in (10)–(19). The indices inside the soft and dark gray area form $\mathcal{G}^{(n)}$ and $\mathcal{C}^{(n)}$ respectively. The indices that form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}$ are those inside the red curve, while those inside the blue curve form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}$.

For sufficiently large n, assumption (3) imposes the following restriction on the size of the previous sets:

$$|\mathcal{G}_1^{(n)}| - |\mathcal{C}_2^{(n)}| \geq |\mathcal{G}_2^{(n)}| - |\mathcal{C}_1^{(n)}| > |\mathcal{C}_{1,2}^{(n)}| - |\mathcal{G}_0^{(n)}|. \tag{20}$$

The left-hand inequality in (20) holds from the fact that

$$\begin{aligned}
&|\mathcal{C}_1^{(n)} \cup \mathcal{G}_1^{(n)}| - |\mathcal{C}_2^{(n)} \cup \mathcal{G}_2^{(n)}| \\
&\quad = \left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}} \setminus \mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}\right| - \left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}} \setminus \mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\right| \\
&\quad = \left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\right| - \left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}\right| \geq 0,
\end{aligned}$$

where the positivity holds by Lemma 4 of [10] because, for any $k \in [1,2]$, we have

$$\frac{1}{n}\left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(k)}}^{(n)})^{\mathrm{C}}\right| = \frac{1}{n}|\mathcal{H}_{V|Y_{(k)}}^{(n)}| + \frac{1}{n}\left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(k)}}^{(n)})^{\mathrm{C}} \setminus \mathcal{H}_{V|Y_{(k)}}^{(n)}\right| \xrightarrow{n\to\infty} H(V|Y_{(k)})$$

Similarly, the right-hand inequality in (20) holds by Lemma 4 of [10] and the fact that

$$\begin{aligned}
|\mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}| - |\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}| &= \left|\mathcal{H}_{V|Z}^{(n)} \setminus \mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\right| - \left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}} \setminus \mathcal{H}_{V|Z}^{(n)}\right| \\
&= |\mathcal{H}_{V|Z}^{(n)}| - \left|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\right|.
\end{aligned}$$

Thus, according to (20), we must consider four cases:

A. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$;
B. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$;
C. $|\mathcal{G}_1^{(n)}| \geq |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| \leq |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$;
D. $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$.

4.1. General Polar-Based Encoding

The generic encoding process for all cases is summarized in Algorithm 1. For $i \in [1, L]$, let W_i be a uniformly distributed vector of length $|\mathcal{C}^{(n)}|$ that represents the private message. The encoder forms

$\tilde{A}_i[\mathcal{C}^{(n)}]$ by simply storing W_i. Indeed, if $i \in [1, L-1]$, notice that the encoder forms $\tilde{A}_{i+1}[\mathcal{C}^{(n)}]$ before constructing $\tilde{A}_i^n$ entirely. From $\tilde{A}_i[\mathcal{C}^{(n)}]$, $i \in [1, L]$, we define

$$\Psi_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_2^{(n)}], \tag{21}$$

$$\Gamma_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_{1,2}^{(n)}], \tag{22}$$

$$\Theta_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_1^{(n)}]. \tag{23}$$

Notice that $[\Psi_i^{(V)}, \Gamma_i^{(V)}] = \tilde{A}_i[\mathcal{C}_2^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ is required by legitimate Receiver 2 to reliably estimate $\tilde{A}_i^n$ and, thus, the encoder will repeat $[\Psi_i^{(V)}, \Gamma_i^{(V)}]$, if $i \in [1, L-1]$, conveniently in $\tilde{A}_{i+1}[\mathcal{G}^{(n)}]$ (the function `form_Ag` is responsible of the chaining construction and is described later). On the other hand, $[\Theta_i^{(V)}, \Gamma_i^{(V)}] = \tilde{A}_i[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ is required by legitimate Receiver 1. Nevertheless, in order to satisfy the strong secrecy condition in (2), $[\Theta_i^{(V)}, \Gamma_i^{(V)}]$, $i \in [2, L]$, is not repeated directly into $\tilde{A}_{i-1}[\mathcal{G}^{(n)}]$, but the encoder copies instead $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ obtained as follows. Let $\kappa_\Theta^{(V)}$ and $\kappa_\Gamma^{(V)}$ be uniformly distributed keys with length $|\mathcal{C}_1^{(n)}|$ and $|\mathcal{C}_{1,2}^{(n)}|$ respectively that are privately shared between transmitter and both legitimate receivers. For any $i \in [2, L]$, we define the sequences

$$\bar{\Theta}_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_1^{(n)}] \oplus \kappa_\Theta^{(V)},$$

$$\bar{\Gamma}_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_{1,2}^{(n)}] \oplus \kappa_\Gamma^{(V)}.$$

Since these secret keys are reused in all blocks, their size becomes negligible in terms of rate for L large enough. The need of these secret keys may not be obvious at this point, but a further discussion of this question can be found in Section 5.4. Indeed, they are required to prove independence between an eavesdropper's observations of adjacent blocks (see Lemma 3), which is crucial to prove that the polar coding scheme satisfies the strong secrecy condition in (2).

Algorithm 1 Generic encoding scheme

Require: Private and confidential messages $W_{1:L}$ and $S_{1:L}$; randomization sequences $R_{1:L}$; random sequence $\Lambda_0^{(X)}$; and secret keys $\kappa_\Theta^{(V)}$, $\kappa_\Gamma^{(V)}$, $\kappa_{\mathrm{Y}\Phi_{(1)}}^{(V)}$ and $\kappa_{\mathrm{Y}\Phi_{(2)}}^{(V)}$.

$\Psi_0^{(V)}, \Gamma_0^{(V)}, \Pi_0^{(V)}, \Lambda_0^{(V)}, \bar{\Theta}_{L+1}^{(V)}, \bar{\Gamma}_{L+1}^{(V)} \leftarrow \varnothing$

$\tilde{A}_1[\mathcal{C}^{(n)}] \leftarrow W_1$

$\Psi_1^{(V)}, \Gamma_1^{(V)} \leftarrow \tilde{A}_1[\mathcal{C}^{(n)}]$

for $i = 1$ to L **do**

  if $i \neq L$ **then**

    $\tilde{A}_{i+1}[\mathcal{C}^{(n)}] \leftarrow W_{i+1}$

    $\Psi_{i+1}^{(V)}, \Gamma_{i+1}^{(V)}, \bar{\Theta}_{i+1}^{(V)}, \bar{\Gamma}_{i+1}^{(V)} \leftarrow \big(\tilde{A}_{i+1}[\mathcal{C}^{(n)}], \kappa_\Theta^{(V)}, \kappa_\Gamma^{(V)}\big)$

  end if

  $\tilde{A}_i\big[\mathcal{G}^{(n)}\big], \Pi_i^{(V)}, \Lambda_i^{(V)} \leftarrow \texttt{form\_A}_{\mathrm{G}}\big(i, S_i, \bar{\Theta}_{i+1}^{(V)}, \bar{\Gamma}_{i+1}^{(V)}, \Psi_{i-1}^{(V)}, \Gamma_{i-1}^{(V)}, \Pi_{i-1}^{(V)}, \Lambda_{i-1}^{(V)}\big)$

  if $i = 1$ **then** $\mathrm{Y}_{(1)}^{(V)} \leftarrow \tilde{A}_1\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$

  if $i = L$ **then** $\mathrm{Y}_{(2)}^{(V)} \leftarrow \tilde{A}_L\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$

  for $j \in \big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}}$ **do**

    if $j \in \big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}$ **then**

      $\tilde{A}_i(j) \leftarrow p_{A(j)|A^{1:j-1}}\big(\tilde{A}_i(j)\big|\tilde{A}_i^{1:j-1}\big)$

    else if $j \in \mathcal{L}_V^{(n)}$ **then**

      $\tilde{A}_i(j) \leftarrow \arg\max_{a \in \mathcal{V}} p_{A(j)|A^{1:j-1}}\big(\tilde{a}_i(j)\big|\tilde{A}_i^{1:j-1}\big)$

    end if

  end for

  $\Phi_{(1),i}^{(V)} \leftarrow \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$

  $\Phi_{(2),i}^{(V)} \leftarrow \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$

  $\tilde{X}_i^n, \Lambda_i^{(X)} \leftarrow \texttt{pb\_ch\_pref}\big(\tilde{A}_i^n G_n, R_i, \Lambda_{i-1}^{(X)}\big)$

end for

Send $\big(\Phi_{(k),i}^{(V)}, \mathrm{Y}_{(k)}^{(V)}\big) \oplus \kappa_{\mathrm{Y}\Phi_{(k)}}^{(V)}$ to Receiver $k \in [1,2]$

return $\tilde{X}_{1:L}^n$

The function `form_A`$_{\mathrm{G}}$ in Algorithm 1 constructs sequences $\tilde{A}_{1:L}[\mathcal{G}^{(n)}]$ differently depending on which case, among cases A, B, C or D described before, characterizes the given CI-WTBC. This part of the encoding is described in detail in Section 4.2 and Algorithm 2.

Then, given $\tilde{A}_i[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}]$, the encoder forms the remaining entries of $\tilde{A}_i^n$, i.e., $\tilde{A}_i[(\mathcal{H}_V^{(n)})^{\mathrm{C}}]$, as follows. If $j \in \mathcal{L}_V^{(n)}$, where $\mathcal{L}_V^{(n)} \triangleq \big\{j \in [1,n] : H\big(A(j)\big|A^{1:j-1}\big) \leq \delta_n\big\}$, it constructs $\tilde{A}_i(j)$ deterministically by using SC encoding [24], and only $\tilde{A}_i[(\mathcal{H}_V^{(n)})^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}]$ is constructed randomly.

Finally, given $\tilde{V}_i^n = \tilde{A}_i^n G_n$, a randomization sequence R_i and a uniformly distributed random sequence $\Lambda_0^{(V)}$, the encoder performs polar-based channel prefixing (function `pb_ch_pref` in Algorithm 1) to obtain $\tilde{X}_i^n$, which is transmitted over the WTBC inducing $\big(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n\big)$. This part of the encoding is described in detail in Section 4.3.

Furthermore, the encoder obtains the sequence

$$\Phi_{(k),i}^{(V)} \triangleq \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big]$$

for any $k \in [1,2]$ and $i \in [1,L]$, which is required by legitimate Receiver k to reliably estimate $\tilde{A}_i^n$ entirely. Since $\Phi_{(k),i}^{(V)}$ is not *nearly uniform*, the encoder cannot make it available to the legitimate Receiver k by means of the chaining structure. Furthermore, the encoder obtains

$$\Upsilon_{(1)}^{(V)} \triangleq \tilde{A}_1\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\big],$$
$$\Upsilon_{(2)}^{(V)} \triangleq \tilde{A}_L\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}\big].$$

The sequence $\Upsilon_{(k)}^{(V)}$ is required by legitimate Receiver $k \in [1,2]$ to initialize the decoding process. Therefore, the transmitter additionally sends $\big(\Upsilon_{(k)}^{(V)}, \Phi_{(k),i}^{(V)}\big) \oplus \kappa_{\Upsilon\Phi_{(k)}}^{(V)}$ to legitimate Receiver k, where $\kappa_{\Upsilon\Phi_{(k)}}^{(V)}$ is a uniformly distributed key with size

$$L\Big|(\mathcal{H}_V^{(n)})^{\mathrm{C}} \cap (\mathcal{L}_{V|Y_{(k)}}^{(n)})^{\mathrm{C}}\Big| + \Big|\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(k)}}^{(n)})^{\mathrm{C}}\Big|$$

that is privately shared between transmitter and the corresponding receiver. In Section 5.1 we show that the length of $\kappa_{\Upsilon\Phi_{(1)}}^{(V)}$ and $\kappa_{\Upsilon\Phi_{(2)}}^{(V)}$ is asymptotically negligible in terms of rate.

Algorithm 2 Function `form_Ag`

Require: i, S_i, $\bar{\Theta}_{i+1}^{(V)}$, $\bar{\Gamma}_{i+1}^{(V)}$, $\Psi_{i-1}^{(V)}$, $\Gamma_{i-1}^{(V)}$, $\Pi_{i-1}^{(V)}$, $\Lambda_{i-1}^{(V)}$

Define $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2^{\prime(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}^{\prime(n)}$, $\mathcal{I}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$, $\mathcal{R}_{\Lambda}^{(n)}$ (depending on the case)
if $i = 1$ **then** $\tilde{A}_1[\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}] \leftarrow S_1$
if $i \in [2, L-1]$ **then** $\tilde{A}_i[\mathcal{I}^{(n)}] \leftarrow S_i$
if $i = L$ **then** $\tilde{A}_L[\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}] \leftarrow S_L$
$\Psi_{1,i-1}^{(V)}, \Psi_{2,i-1}^{(V)} \leftarrow \Psi_{i-1}^{(V)}$ (depending on the case)
$\Gamma_{1,i-1}^{(V)}, \Gamma_{2,i-1}^{(V)} \leftarrow \Gamma_{i-1}^{(V)}$ (depending on the case)
$\bar{\Theta}_{1,i+1}^{(V)}, \bar{\Theta}_{2,i+1}^{(V)} \leftarrow \bar{\Theta}_{i+1}^{(V)}$ (depending on the case)
$\bar{\Gamma}_{1,i+1}^{(V)}, \bar{\Gamma}_{2,i+1}^{(V)} \leftarrow \bar{\Gamma}_{i+1}^{(V)}$ (depending on the case)
$\tilde{A}_i[\mathcal{R}_{1,2}^{(n)}] \leftarrow \Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$
$\tilde{A}_i[\mathcal{R}_{1,2}^{\prime(n)}] \leftarrow \Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$
if $i \in [1, L-1]$ **then**
    $\tilde{A}_i[\mathcal{R}_1^{(n)}] \leftarrow \bar{\Theta}_{1,i+1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_1^{\prime(n)}] \leftarrow \bar{\Gamma}_{2,i+1}^{(V)}$
end if
if $i \in [2, L]$ **then**
    $\tilde{A}_i[\mathcal{R}_2^{(n)}] \leftarrow \Psi_{1,i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_2^{\prime(n)}] \leftarrow \Gamma_{2,i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}] \leftarrow \Pi_{i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}] \leftarrow \Lambda_{i-1}^{(V)}$
end if
$\Pi_i^{(V)} \leftarrow \tilde{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$
$\Lambda_i^{(V)} \leftarrow \tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$
return the sequences $\tilde{A}_i\big[\mathcal{G}^{(n)}\big]$, $\Pi_i^{(V)}$ and $\Lambda_i^{(V)}$

4.2. Function `form_Ag`

The function `form_Ag` encodes the confidential messages $S_{1:L}$ and builds the chaining construction. Based on the sets in (10)–(19), let $\mathcal{R}_1^{(n)} \subseteq \mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}$, $\mathcal{R}_1'^{(n)} \subseteq \mathcal{G}_2^{(n)}$, $\mathcal{R}_2^{(n)} \subseteq \mathcal{G}_1^{(n)}$, $\mathcal{R}_2'^{(n)} \subseteq \mathcal{G}_1^{(n)}$, $\mathcal{R}_{1,2}^{(n)} \subseteq \mathcal{G}_0^{(n)}$, $\mathcal{R}_{1,2}'^{(n)} \subseteq \mathcal{G}_0^{(n)}$, $\mathcal{I}^{(n)} \subseteq \mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)} \subseteq \mathcal{G}_1^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)} \subseteq \mathcal{G}_1^{(n)}$ form an additional partition of $\mathcal{G}^{(n)}$. The definition of $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_{1,2}'^{(n)}$ will depend on the particular case (among A to D), while

$$\mathcal{I}^{(n)} \triangleq \left(\mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}\right) \setminus \left(\mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)} \cup \mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}'^{(n)}\right), \tag{24}$$

$$\mathcal{R}_{\mathrm{S}}^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\right) \text{ with size } \left|\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right|, \tag{25}$$

$$\mathcal{R}_{\Lambda}^{(n)} \triangleq \mathcal{G}_{1,2}^{(n)} \cup \left(\mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\mathrm{S}}^{(n)}\right)\right). \tag{26}$$

For $i \in [1, L]$, let S_i denote a uniformly distributed vector that represents the confidential message. The message S_1 has size $\left|\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}\right|$; for $i \in [2, L-1]$, S_i has size $\left|\mathcal{I}^{(n)}\right|$; and S_L has size $\left|\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}\right|$. Furthermore, for $i \in [1, L]$, we write $\Psi_i^{(V)} \triangleq \left[\Psi_{1,i}^{(V)}, \Psi_{2,i}^{(V)}\right]$, $\Gamma_i^{(V)} \triangleq \left[\Gamma_{1,i}^{(V)}, \Gamma_{2,i}^{(V)}\right]$, $\bar{\Theta}_i^{(V)} \triangleq \left[\bar{\Theta}_{1,i}^{(V)}, \bar{\Theta}_{2,i}^{(V)}\right]$ and $\bar{\Gamma}_i^{(V)} \triangleq \left[\bar{\Gamma}_{1,i}^{(V)}, \bar{\Gamma}_{2,i}^{(V)}\right]$, where we define $\Psi_{p,i}$, $\Gamma_{p,i}$, $\bar{\Theta}_{p,i}$ and $\bar{\Gamma}_{p,i}$, for any $p \in [1, 2]$, accordingly in each case.

This function, which is used in Case A to Case D, is described in Algorithm 2.

4.2.1. Case A

In this case, recall that $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$. We define

$$\mathcal{R}_1^{(n)} \triangleq \text{any subset of } \mathcal{G}_2^{(n)} \text{ with size } \left|\mathcal{C}_1^{(n)}\right|, \tag{27}$$

$$\mathcal{R}_2^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \left|\mathcal{C}_2^{(n)}\right|, \tag{28}$$

$$\mathcal{R}_{1,2}^{(n)} \triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \left|\mathcal{C}_{1,2}^{(n)}\right|, \tag{29}$$

and $\mathcal{R}_1'^{(n)} = \mathcal{R}_2'^{(n)} = \mathcal{R}_{1,2}'^{(n)} \triangleq \varnothing$. By the assumption of Case A, it is clear that $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$ and $\mathcal{R}_{1,2}^{(n)}$ exist. Furthermore, by (20), the set $\mathcal{I}^{(n)}$ exists, and so will $\mathcal{R}_{\mathrm{S}}^{(n)}$ because

$$\begin{aligned}\left|\mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\right)\right| - \left|\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right| &= \left|\mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\right)\right| - \left|\left(\mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)}\right)\right| \\ &= \left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| \geq 0.\end{aligned}$$

These sets that form the partition of $\mathcal{G}^{(n)}$ in Case A can be seen in Figure 3, which also displays the encoding process that aims to construct $\tilde{A}_{1:L}\left[\mathcal{H}_V^{(n)}\right] = \tilde{A}_{1:L}\left[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}\right]$.

For $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and, therefore, we have $\Psi_{2,i}^{(V)} = \Gamma_{2,i}^{(V)} = \bar{\Theta}_{2,i}^{(V)} = \bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$.

From (18), we have $\mathcal{C}_2^{(n)} \subseteq \mathcal{L}_{V|Y_{(1)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(2)}}^{(n)}$. Thus, the sequence $\Psi_{1,i-1}^{(V)} = \tilde{A}_{i-1}\left[\mathcal{C}_2^{(n)}\right]$ is needed by legitimate Receiver 2 to reliably reconstruct $\tilde{A}_{i-1}^n$, but can be reliably inferred by legitimate Receiver 1 given $\tilde{A}_{i-1}\left[\left(\mathcal{L}_{V|Y_{(1)}}^{(n)}\right)^{\mathrm{C}}\right]$. Hence, according to Algorithm 2, the encoder repeats the entire sequence $\Psi_{1,i-1}^{(V)}$ in $\tilde{A}_i\left[\mathcal{R}_2^{(n)}\right] \subseteq \tilde{A}_i\left[\mathcal{L}_{V|Y_{(2)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}\right]$.

Similarly, from (17), we have $\mathcal{C}_1^{(n)} \subseteq \mathcal{L}_{V|Y_{(2)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}$. Thus, $\Theta_{1,i+1}^{(V)} = \tilde{A}_{i+1}\left[\mathcal{C}_1^{(n)}\right]$ is needed by Receiver 1 to form $\tilde{A}_{i+1}^n$ but can be inferred by Receiver 2 given $\tilde{A}_{i+1}\left[\left(\mathcal{L}_{V|Y_{(2)}}^{(n)}\right)^{\mathrm{C}}\right]$. Hence, the encoder repeats the sequence $\bar{\Theta}_{1,i+1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_1^{(n)}] \subseteq \tilde{A}_i\left[\mathcal{L}_{V|Y_{(1)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(2)}}^{(n)}\right]$.

Finally, from (19), $\mathcal{C}_{1,2}^{(n)} \subseteq (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}$. Thus, sequences $\Gamma_{1,i-1}^{(V)} = \tilde{A}_{i-1}[\mathcal{C}_{1,2}^{(n)}]$ and $\Gamma_{1,i+1}^{(V)} = \tilde{A}_{i+1}[\mathcal{C}_{1,2}^{(n)}]$ are needed by both receivers to form $\tilde{A}_{i-1}^{n}$ and $\tilde{A}_{i+1}^{n}$ respectively. Hence, the encoder repeats $\Gamma_{1,i-1}^{(V)}$ and $\bar{\Gamma}_{1,i+1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{1,2}^{(n)}] \subseteq \tilde{A}_i[\mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}]$. Indeed, both sequences are repeated in the same entries of $\tilde{A}_i[\mathcal{G}_0^{(n)}]$ by performing $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. Since $\Gamma_{1,0}^{(V)} = \bar{\Gamma}_{1,L+1}^{(V)} = \varnothing$, only $\bar{\Gamma}_{1,2}^{(V)}$ is repeated at Block 1 and $\Gamma_{1,L-1}^{(V)}$ at Block L.

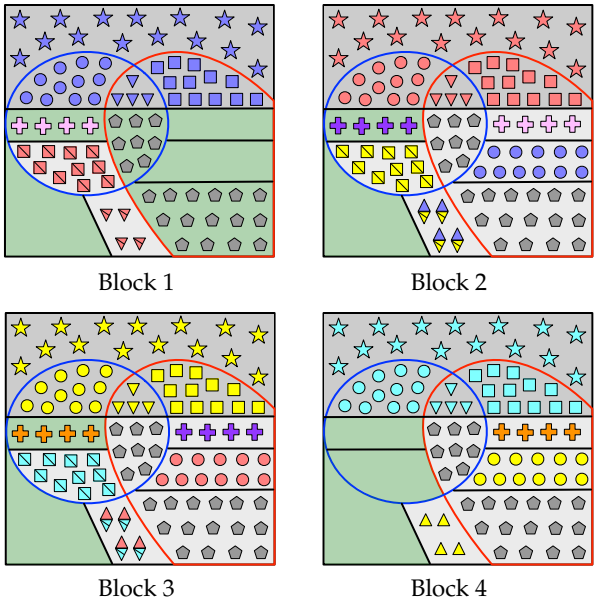

Figure 3. For Case A, graphical representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Block 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, pink crosses, and gray pentagons, respectively, and the set $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Furthermore, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. In Block $i \in [1, L]$, S_i is stored into those entries whose indices belong to the green area. For $i \in [1, L-1]$, $\Pi_i^{(V)}$ is denoted by crosses (e.g., purple crosses at Block 2), and is repeated in $\tilde{A}_{i+1}[\mathcal{R}_{\mathrm{S}}^{(n)}]$. The sequence $\Lambda_1^{(V)}$ is represented by gray pentagons and is replicated in all blocks. The sequences $\mathrm{Y}_{(1)}^{(V)}$ and $\mathrm{Y}_{(2)}^{(V)}$ are those entries inside the red at Block 1 and the blue curve at Block L, respectively.

Moreover, part of secret message S_i, $i \in [1, L]$, is stored into some entries of $\tilde{A}_i^n$ whose indices belong to $\mathcal{G}_2^{(n)}$. Thus, in any Block $i \in [2, L]$, the encoder repeats

$$\Pi_{i-1}^{(V)} \triangleq \tilde{A}_{i-1}[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$$

in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}] \subseteq \tilde{A}_i[\mathcal{L}_{V|Y_{(2)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}]$. Furthermore, it repeats

$$\Lambda_{i-1}^{(V)} \triangleq \tilde{A}_{i-1}[\mathcal{R}_{\Lambda}^{(n)}]$$

in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$. Hence, notice that $\Lambda_1^{(V)}$ is replicated in all blocks.

4.2.2. Case B

In this case, $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$. We define $\mathcal{R}_1^{(n)}$ and $\mathcal{R}_2^{(n)}$ as in (27) and (28) respectively, and $\mathcal{R}_{1,2}^{\prime(n)} \triangleq \emptyset$. Now, since $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$, only a part of $\Gamma_{i-1}^{(V)}$ and $\bar{\Gamma}_{i+1}^{(V)}$, $i \in [1, L]$, can be repeated in $\tilde{A}_i[\mathcal{G}_0^{(n)}]$. Thus, we define $\mathcal{R}_{1,2}^{(n)} \triangleq \mathcal{G}_0^{(n)}$ and

$$\mathcal{R}_1^{\prime(n)} \triangleq \text{any subset of } \mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \text{ with size } |\mathcal{C}_{1,2}^{(n)}| - |\mathcal{G}_0^{(n)}|, \tag{30}$$

$$\mathcal{R}_2^{\prime(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } |\mathcal{C}_{1,2}^{(n)}| - |\mathcal{G}_0^{(n)}|. \tag{31}$$

Obviously, $\mathcal{R}_{1,2}^{(n)}$ exists and, by the assumption of Case B, so do $\mathcal{R}_1^{(n)}$ and $\mathcal{R}_2^{(n)}$. By (20), $\mathcal{R}_1^{\prime(n)}$ exists and so does $\mathcal{I}^{(n)}$. Indeed, since $\mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} = \emptyset$, then $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$. Again, by the property in (20), $\mathcal{R}_2^{\prime(n)}$ exists and so does $\mathcal{R}_{\mathrm{S}}^{(n)}$ because

$$\begin{aligned}
&|\mathcal{G}_1^{(n)} \setminus (\mathcal{R}_2^{(n)} \cup \mathcal{R}_2^{\prime(n)})| - |(\mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \cup \mathcal{R}_1^{\prime(n)})| \\
&\quad = |\mathcal{G}_1^{(n)}| - |\mathcal{C}_2^{(n)}| - (|\mathcal{C}_{1,2}^{(n)}| - |\mathcal{G}_0^{(n)}|) - \left(|\mathcal{G}_2^{(n)}| - |\mathcal{C}_1^{(n)}| - (|\mathcal{C}_{1,2}^{(n)}| - |\mathcal{G}_0^{(n)}|)\right) \\
&\quad = |\mathcal{G}_1^{(n)}| - |\mathcal{C}_2^{(n)}| - |\mathcal{G}_2^{(n)}| + |\mathcal{C}_1^{(n)}| \geq 0.
\end{aligned}$$

Indeed, since $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$, notice that $|\mathcal{R}_{\mathrm{S}}^{(n)}| = |\mathcal{I}^{(n)}|$. These sets that form the partition of $\mathcal{G}^{(n)}$ in Case B can be seen in Figure 4, which also displays the encoding process that aims to construct $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}] = \tilde{A}_{1:L}[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}]$.

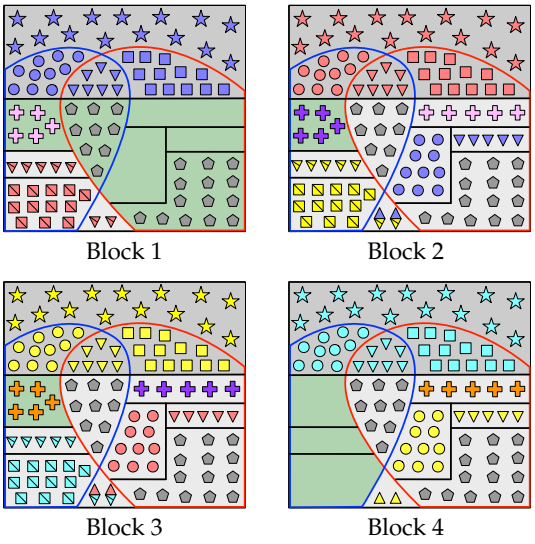

Figure 4. For Case B, graphical representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2^{\prime(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, yellow triangles, blue circles, blue triangles, blue and yellow diamonds, pink crosses, and gray pentagons, respectively, and $\mathcal{I}^{(n)}$ is the green filled area with purple crosses. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles, and triangles, respectively. Furthermore, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. In Block $i \in [1, L]$, S_i is stored into those entries whose indices belong to the green area. For $i \in [2, L-1]$, $\Pi_i^{(V)} = S_i$ and, therefore, S_i is repeated entirely into $\tilde{A}_{i+1}[\mathcal{R}_{\mathrm{S}}^{(n)}]$. The sequence $\Lambda_1^{(V)}$ from S_1 is represented by gray pentagons and is repeated in all blocks. The sequences $\mathrm{Y}_{(1)}^{(V)}$ and $\mathrm{Y}_{(2)}^{(V)}$ are the entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

In this case, for any $i \in [1, L]$, $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$ and $\Psi_{2,i}^{(V)} = \bar{\Theta}_{2,i}^{(V)} \triangleq \varnothing$; and we define $\Gamma_{1,i}^{(V)}$ and $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$, respectively, with size $|\mathcal{G}_0^{(n)}|$, and $\Gamma_{2,i}^{(V)}$ and $\bar{\Gamma}_{2,i}^{(V)}$ as the remaining parts with size $|\mathcal{C}_{1,2}^{(n)}| - |\mathcal{G}_0^{(n)}|$. Now, the encoder copies $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$ into $\tilde{A}_i[\mathcal{R}_{1,2}^{(n)}]$, and $\Gamma_{2,i-1}^{(V)}$ and $\bar{\Gamma}_{2,i+1}^{(V)}$ into $\tilde{A}_i[\mathcal{R}_2'^{(n)}]$ and $\tilde{A}_i[\mathcal{R}_1'^{(n)}]$ respectively. Moreover, since $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$, notice that $\Pi_i^{(V)} = S_i$ for any $i \in [2, L-1]$.

4.2.3. Case C

In this case, recall that $|\mathcal{G}_1^{(n)}| \geq |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| \leq |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$. Hence, we define $\mathcal{R}_2^{(n)}$ and $\mathcal{R}_{1,2}^{(n)}$ as in (28) and (29) respectively, and $\mathcal{R}_1'^{(n)} = \mathcal{R}_2'^{(n)} = \mathcal{R}_{1,2}'^{(n)} \triangleq \varnothing$. On the other hand, since $|\mathcal{G}_2^{(n)}| \leq |\mathcal{C}_1^{(n)}|$, now for $i \in [1, L-1]$ only a part of $\bar{\Theta}_{i+1}^{(V)}$ can be repeated entirely in $\tilde{A}_i[\mathcal{G}_2^{(n)}]$. Consequently, we define

$$\mathcal{R}_1^{(n)} \triangleq \text{the union of } \mathcal{G}_2^{(n)} \text{ with any subset of } \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} \text{ with size } |\mathcal{C}_1^{(n)}| - |\mathcal{G}_2^{(n)}|. \tag{32}$$

It is clear that $\mathcal{R}_2^{(n)}$ and $\mathcal{R}_{1,2}^{(n)}$ exist. By (20), $\mathcal{R}_1^{(n)}$ also exists and so does $\mathcal{I}^{(n)}$. Since $\mathcal{R}_1^{(n)} \supseteq \mathcal{G}_2^{(n)}$, then $\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)} = \varnothing$ and $\mathcal{R}_S^{(n)} = \varnothing$. These sets that form $\mathcal{G}^{(n)}$ are represented in Figure 5, which also displays the part of the encoding that aims to construct $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$.

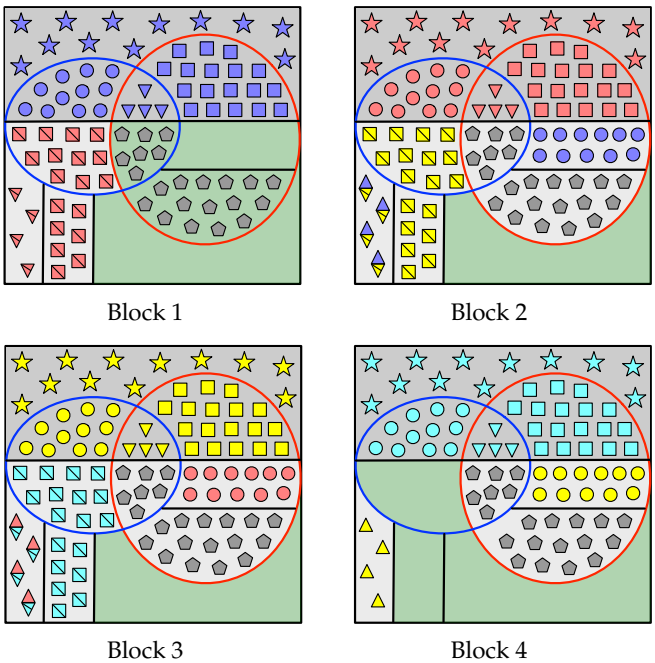

Figure 5. For Case C, graphical representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Bloc 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_\Lambda^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, and gray pentagons, respectively, and $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles, and triangles, respectively. Furthermore, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. For $i \in [1, L]$, S_i is stored into those entries belonging to the green area. The sequence $\Lambda_1^{(V)}$ is represented by gray pentagons and is repeated in all blocks. The sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are the entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

In this case, for $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$, and $\Psi_{2,i}^{(V)} = \Gamma_{2,i}^{(V)} = \bar{\Theta}_{2,i}^{(V)} = \bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$. Moreover, note that $\Pi_i^{(V)} = \varnothing$ because $\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)} = \emptyset$.

4.2.4. Case D

In this case, recall that $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$. The sets that form the partition of $\mathcal{G}^{(n)}$ in Case D are defined below and can be seen in Figure 6, which also displays the encoding process that aims to construct of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$.

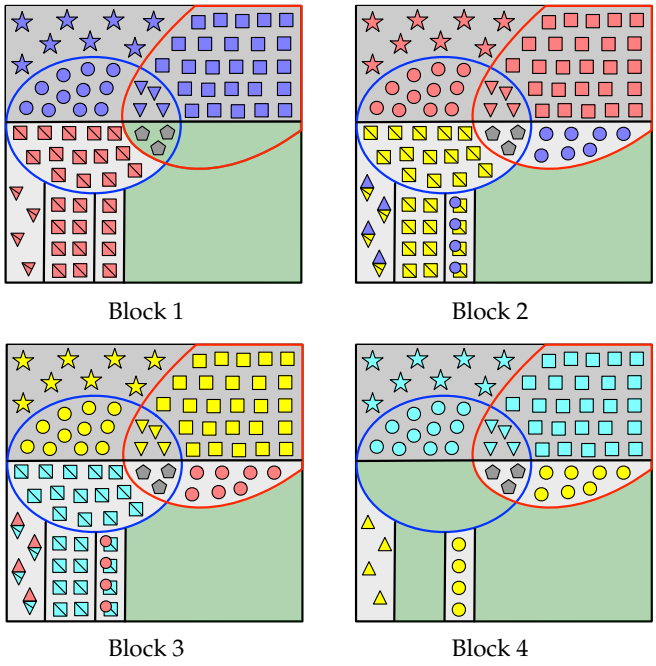

Figure 6. For Case D, graphical representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Block 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}^{\prime(n)}$ and $\mathcal{R}_\Lambda^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, yellow squares overlapped by blue circles, and gray pentagons, respectively, and the set $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles, and triangles, respectively. Furthermore, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$ is represented by diamonds, and $\Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$ by squares overlapped by circles. At Block $i \in [1, L]$, S_i is stored into those entries that belong to the green area. Sequence $\Lambda_1^{(V)}$ is denoted by gray pentagons and is repeated in all blocks. Sequences $\mathrm{Y}_{(1)}^{(V)}$ and $\mathrm{Y}_{(2)}^{(V)}$ are the entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

As in Case A and Case C, since $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$ then we define the set $\mathcal{R}_{1,2}^{(n)}$ as in (29) and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} \triangleq \varnothing$. On the other hand, since $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, now for $i \in [2, L]$ only a part of $\Psi_{i-1}^{(V)}$ can be repeated entirely in $\tilde{A}_i[\mathcal{G}_1^{(n)}]$. Consequently, we define $\mathcal{R}_2^{(n)} \triangleq \mathcal{G}_1^{(n)}$ and

$$\mathcal{R}_{1,2}^{\prime(n)} \triangleq \text{any subset of } \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} \text{ with size } |\mathcal{C}_2^{(n)}| - |\mathcal{G}_1^{(n)}|. \tag{33}$$

By (20), it is clear that $\mathcal{R}_{1,2}^{\prime(n)}$ exists. Now, despite $\left|\mathcal{G}_2^{(n)}\right| < \left|\mathcal{C}_1^{(n)}\right|$ as in Case C, the set $\mathcal{R}_1^{(n)}$ is not defined as in (32), but

$$\mathcal{R}_1^{(n)} \triangleq \text{the union of } \mathcal{G}_2^{(n)} \text{ with any subset of } \mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right) \text{ with size } \left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right), \tag{34}$$

which exists because, by the assumption in (20), we have

$$\begin{aligned}
&\left|\mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right)\right| - \left|\mathcal{R}_1^{(n)}\right| \\
&= \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| + \left|\mathcal{G}_1^{(n)}\right| - \left(\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| + \left|\mathcal{G}_1^{(n)}\right|\right) \\
&= \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| + \left|\mathcal{G}_2^{(n)}\right| \geq 0.
\end{aligned}$$

In this case, for $i \in [1, L]$, we set $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\bar{\Gamma}_{2,i}^{(V)} = \Gamma_{2,i}^{(V)} \triangleq \varnothing$. Furthermore, we define $\Psi_{1,i}^{(V)}$ as any part of $\Psi_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, and $\Psi_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$. Lastly, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right)$, and $\bar{\Theta}_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$.

Thus, according to Algorithm 2, instead of repeating $\Psi_{2,i-1}^{(V)}$, that is, the part of $\Psi_{i-1}^{(V)}$ that does not fit in $\tilde{A}_i^n\left[\mathcal{G}_1^{(n)}\right]$, in a specific part of $\tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$, the encoder stores $\Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$ into $\tilde{A}_i\left[\mathcal{R}_{1,2}^{\prime(n)}\right] \subseteq \tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$, where $\bar{\Theta}_{2,i+1}^{(V)}$ denotes part of those elements of $\bar{\Theta}_{i+1}^{(V)}$ that do not fit in $\tilde{A}_i\left[\mathcal{G}_2^{(n)}\right]$. Furthermore, as in Case C, since $\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)} = \emptyset$, we have $\Pi_i^{(V)} = \varnothing$.

4.3. Channel Prefixing

For $i \in [1, L]$, let R_i be a uniformly distributed vector of length $\left|\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right|$ that represents the randomization sequence. Furthermore, let $\Lambda_0^{(X)}$ be a uniformly distributed random sequence of size $\left|\mathcal{H}_{X|VZ}^{(n)}\right|$. The channel prefixing aims to construct $\tilde{X}_i^n = \tilde{T}_i^n G_n$ and is summarized in Algorithm 3.

Algorithm 3 Function `pb_ch_pref`

Require: $\tilde{V}_i^n$, R_i, $\Lambda_{i-1}^{(X)}$
1: $\tilde{T}_i\left[\mathcal{H}_{X|VZ}^{(n)}\right] \leftarrow \Lambda_{i-1}^{(X)}$
2: $\tilde{T}_i\left[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right] \leftarrow R_i$
3: **for** $j \in \left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}}$ **do**
4: **if** $j \in \left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}$ **then**
5: $\tilde{T}_i(j) \leftarrow p_{T(j)|T^{1:j-1}V^n}\left(\tilde{T}_i(j) \middle| \tilde{T}_i^{1:j-1}\tilde{V}_i^n\right)$
6: **else if** $j \in \mathcal{L}_{X|V}^{(n)}$ **then**
7: $\tilde{T}_i(j) \leftarrow \arg\max_{t \in \mathcal{X}} p_{T(j)|T^{1:j-1}V^n}\left(t \middle| \tilde{T}_i^{1:j-1}\tilde{V}_i^n\right)$
8: **end if**
9: **end for**
10: $\tilde{X}_i^n \leftarrow \tilde{T}_i^n G_n$
11: $\Lambda_i^{(X)} \leftarrow \tilde{T}_i\left[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right]$
12: **return** $\tilde{X}_i^n$ and $\Lambda_i^{(X)}$

Notice that the sequence $\Lambda_0^{(X)}$ is copied in $\tilde{T}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]$ at any Block $i \in [1, L]$, while R_i is stored into $\tilde{T}_i\big[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\big]$. After forming $\tilde{T}_i\big[\mathcal{H}_{X|V}^{(n)}\big]$, and given the sequence $\tilde{V}_i^n \triangleq \tilde{A}_i^n G_n$, the encoder forms the remaining entries of $\tilde{T}_i^n$, that is, $\tilde{T}_i\big[\big(\mathcal{H}_{X|V}^{(n)}\big)^{\mathrm{C}}\big]$ as follows. If $j \in \mathcal{L}_{X|V}^{(n)}$, where $\mathcal{L}_{V|X}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T(j)\big|T^{1:j-1}V^n\big) \leq \delta_n\big\}$, it constructs $\tilde{T}_i(j)$ deterministically by using SC encoding [24]. Otherwise, if $j \in \big(\mathcal{H}_{X|V}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}$, the encoder randomly draws $\tilde{T}_i(j)$ from distribution $p_{T(j)|T^{1:j-1}V^n}$.

4.4. Decoding

Consider that $\big(\mathrm{Y}_{(k)}^{(V)}, \Phi_{(k),1:L}^{(V)}\big)$, for all $k \in [1,2]$, is available to the k-th legitimate receiver. In the decoding process, both legitimate receivers form the estimates $\hat{A}_{1:L}^n$ of $\tilde{A}_{1:L}^n$ and then obtain the messages $\big(\hat{W}_{1:L}, \hat{S}_{1:L}\big)$.

4.4.1. Legitimate Receiver 1

This receiver forms the estimates $\hat{A}_{1:L}^n$ by going forward, i.e., from $\hat{A}_1^n$ to $\hat{A}_L^n$, and this process is summarized in Algorithm 4.

Algorithm 4 Decoding at legitimate Receiver 1

Require: $\mathrm{Y}_{(1)}^{(V)}, \Phi_{(1),1:L}^{(V)}, \kappa_\Theta^{(V)}$ and $\kappa_\Gamma^{(V)}$, and $\tilde{Y}_{(1),1:L}^n$.

$\hat{A}_1^n \leftarrow \big(\mathrm{Y}_{(1)}^{(V)}, \Phi_{(1),1}^{(V)}, \tilde{Y}_{(1),1}^n\big)$
$\hat{\Lambda}_{2:L}^{(V)} \leftarrow \hat{A}_1\big[\mathcal{R}_\Lambda^{(n)}\big]$
for $i = 1$ to $L-1$ **do**
  $\hat{\Psi}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_2^{(n)}]$
  $\hat{\Gamma}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}]$
  $\hat{\tilde{\Theta}}_{i+1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_1^{(n)}], \hat{A}_i[\mathcal{R}_{1,2}^{\prime(n)}] \oplus \hat{\Psi}_{2,i-1}^{(V)}\big)$
  $\hat{\Theta}_{i+1}^{(V)} \leftarrow \hat{\tilde{\Theta}}_{i+1}^{(V)} \oplus \kappa_\Theta^{(V)}$
  $\hat{\tilde{\Gamma}}_{i+1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\Gamma}_{1,i-1}^{(V)}, \hat{A}_i[\mathcal{R}_1^{\prime(n)}]\big)$
  $\hat{\Gamma}_{i+1}^{(V)} \leftarrow \hat{\tilde{\Gamma}}_{i+1}^{(V)} \oplus \kappa_\Gamma^{(V)}$
  $\hat{\Pi}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$
  $\hat{\mathrm{Y}}_{(1),i+1}^{\prime(V)} \leftarrow \big(\hat{\Psi}_{1,i}^{(V)}, \hat{\Gamma}_{2,i}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Pi}_i^{(V)}, \hat{\Lambda}_i^{(V)}\big)$
  $\hat{A}_{i+1}^n \leftarrow \big(\hat{\mathrm{Y}}_{(1),i+1}^{\prime(V)}, \Phi_{(1),i+1}^{(V)}, \tilde{Y}_{(1),i+1}^n\big)$
end for

In all cases (among Case A to Case D), Receiver 1 constructs $\hat{A}_1^n$ as follows. Given $\mathrm{Y}_{(1)}^{(V)}$ (all the elements inside the red curve at Block 1 in Figures 3–6) and $\Phi_{(1),1}^{(V)}$, notice that Receiver 1 knows $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$. Therefore, from $\big(\mathrm{Y}_{(1)}^{(V)}, \Phi_{(1),1}^{(V)}\big)$ and channel observations $\tilde{Y}_{(1),1}^n$, Receiver 1 performs SC decoding to form $\hat{A}_1^n$. Moreover, since $\Lambda_1^{(V)}$ has been replicated in all blocks, legitimate Receiver 1 obtains $\hat{\Lambda}_{2:L}^{(V)} = \hat{A}_1\big[\mathcal{R}_\Lambda^{(n)}\big]$ (gray pentagons in all blocks).

For $i \in [1, L-1]$, consider the construction of $\hat{A}_{i+1}^n$. First, since $\hat{A}_{1:i}^n$ have already been estimated, from $\hat{A}_i^n$ Receiver 1 obtains $\hat{\Psi}_i^{(V)} = \hat{A}_i\big[\mathcal{C}_2^{(n)}\big]$ (e.g., red circles at Block 2 in Figures 3–6) and $\hat{\Gamma}_i^{(V)} = \hat{A}_i\big[\mathcal{C}_{1,2}^{(n)}\big]$ (red triangles).

Furthermore, from $\hat{A}_i^n$, Receiver 1 obtains $\hat{\Theta}_{i+1}^{(V)}$ as follows. At Block 1, in all cases it gets $\hat{\tilde{\Theta}}_2^{(V)} = \tilde{A}_1\big[\mathcal{R}_1^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\big]$ (all the red squares with a line through them at Block 1 in Figures 3–6). At Block $i \in [2, L-1]$, we distinguish two situations:

- In Case D, Receiver 1 gets $\hat{\tilde{\Theta}}_{1,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_1^{(V)}\big]$ (e.g., yellow squares with a line through them at Block 2 in Figure 6) and $\hat{\Psi}_{2,i-1}^{\prime(V)} \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{\prime(V)}\big]$ (yellow squares with a line through them overlapped by blue circles). Since $\hat{\Psi}_{2,i-1}^{(V)} \subset \hat{A}_{i-1}^n$ (blue circles) has already been estimated, Receiver 1 obtains $\hat{\tilde{\Theta}}_{2,i+1}^{(V)} = \hat{\Psi}_{2,i-1}^{(V)} \oplus \hat{A}_i\big[\mathcal{R}_{1,2}^{\prime(V)}\big]$ (yellow squares with a line through them).
- Otherwise, in other cases, Receiver 1 obtains $\hat{\tilde{\Theta}}_{i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_1^{(n)}\big]$ directly (yellow squares with a line through them at Block 2 in Figures 3–5).

Then, given $\hat{\tilde{\Theta}}_{i+1}^{(V)} = \big[\hat{\tilde{\Theta}}_{1,i+1}^{(V)}, \hat{\tilde{\Theta}}_{2,i+1}^{(V)}\big]$, in all cases Receiver 1 recovers $\hat{\Theta}_{i+1}^{(V)} = \hat{\tilde{\Theta}}_{i+1}^{(V)} \oplus \kappa_\Theta^{(V)}$.

From $\hat{A}_i^n$, Receiver 1 also obtains $\hat{\Gamma}_{i+1}^{(V)}$ as follows. At Block 1, in all cases it gets $\hat{\tilde{\Gamma}}_2^{(V)} = \tilde{A}_1\big[\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_1^{\prime(n)}\big]$ directly (e.g., all red triangles with a line through them at Block 1 in Figures 3–6). At Block $i \in [2, L-1]$, in all cases it obtains $\hat{\Gamma}_{1,i-1}^{(V)} \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big]$ (e.g., blue and yellow diamonds with a line through them at Block 2). Since $\hat{\Gamma}_{1,i-1}^{(V)} \subset \hat{A}_{i-1}^n$ (blue triangles) has already been estimated, Receiver 1 obtains $\hat{\tilde{\Gamma}}_{1,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big] \oplus \hat{\Gamma}_{1,i-1}^{(V)}$ (yellow triangles with a line through them). Only in Case B, Receiver 1 obtains $\hat{\tilde{\Gamma}}_{2,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_1^{\prime(n)}\big]$ (remaining yellow triangles with a line through them at Block 2 in Figure 4). Then, given $\hat{\tilde{\Gamma}}_{i+1}^{(V)} = \big[\hat{\tilde{\Gamma}}_{1,i+1}^{(V)}, \hat{\tilde{\Gamma}}_{2,i+1}^{(V)}\big]$, in all cases Receiver 1 recovers $\hat{\Gamma}_{i+1}^{(V)} = \hat{\tilde{\Gamma}}_{i+1}^{(V)} \oplus \kappa_\Gamma^{(V)}$.

Lastly, only in Case A and Case B, Receiver 1 obtains $\hat{\Pi}_i^{(V)} = \hat{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big]$ (e.g., purple crosses at Block 2 in Figure 3 and Figure 4).

Finally, define the sequence $\hat{\Upsilon}_{(1),i+1}^{\prime(V)} \triangleq \big[\hat{\Psi}_{1,i}^{(V)}, \hat{\Gamma}_{2,i}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Pi}_i^{(V)}, \hat{\Lambda}_i^{(V)}\big]$. Notice that $\hat{\Upsilon}_{(1),i+1}^{\prime(V)} \supseteq \hat{A}_{i+1}\big[\mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}\big]$ (elements inside red curve at Block $i+1$ in Figures 3–6). Therefore, Receiver 1 performs SC decoding to form $\hat{A}_{i+1}^n$ by using $\hat{\Upsilon}_{(1),i+1}^{\prime(V)}$, $\Phi_{(1),i+1}^{(V)}$ and the channel observations $\tilde{Y}_{(1),i+1}^n$.

4.4.2. Legitimate Receiver 2

This receiver forms the estimates $\hat{A}_{1:L}^n$ by going backward, i.e., from $\hat{A}_L^n$ to $\hat{A}_1^n$, and this process is summarized in Algorithm 5.

Algorithm 5 Decoding at legitimate Receiver 2

Require: $Y_{(2)}^{(V)}$, $\Phi_{(2),1:L}^{(V)}$, $\kappa_\Theta^{(V)}$ and $\kappa_\Gamma^{(V)}$, and $\tilde{Y}_{(2),1:L}^n$.

$\hat{A}_L^n \leftarrow \big(Y_{(2)}^{(V)}, \Phi_{(2),L}^{(V)}, \tilde{Y}_{(2),L}^n\big)$
$\hat{\Lambda}_{1:L-1}^{(V)} \leftarrow \hat{A}_L\big[\mathcal{R}_\Lambda^{(n)}\big]$
for $i = L$ to 2 **do**
  $\hat{\tilde{\Theta}}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_1^{(n)}] \oplus \kappa_\Theta^{(V)}$
  $\hat{\tilde{\Gamma}}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}] \oplus \kappa_\Gamma^{(V)}$
  $\hat{\Psi}_{i-1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_2^{(n)}], \hat{A}_i[\mathcal{R}_{1,2}^{\prime(n)}] \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)}\big)$
  $\hat{\Gamma}_{i-1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)}, \hat{A}_i[\mathcal{R}_2^{\prime(n)}]\big)$
  $\hat{\Pi}_{i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_S^{(n)}]$
  $\Upsilon_{(2),i-1}^{\prime(V)} \leftarrow \big(\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Pi}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\big)$
  $\hat{A}_{i-1}^n \leftarrow \big(\Upsilon_{(2),i-1}^{\prime(V)}, \Phi_{(2),i-1}^{(V)}, \tilde{Y}_{(2),i-1}^n\big)$
end for

In all cases (among Case A to Case D), Receiver 2 constructs $\hat{A}_L^n$ as follows. Given $Y_{(2)}^{(V)}$ (all the elements inside blue curve at Block 4 in Figures 3–6) and $\Phi_{(2),L}^{(V)}$, notice that Receiver 2 knows $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$. Hence, from $\big(Y_{(2)}^{(V)}, \Phi_{(2),L}^{(V)}\big)$ and channel output observations $\tilde{Y}_{(2),L}^n$, Receiver 2

performs SC decoding to form $\hat{A}_L^n$. Since $\Lambda_1^{(V)}$ has been replicated in all blocks, from $\hat{A}_L^n$ it obtains $\hat{\Lambda}_{1:L-1}^{(V)} = \hat{A}_L\big[\mathcal{R}_\Lambda^{(n)}\big]$ (gray pentagons at all blocks).

For $i \in [2, L]$, consider the construction of $\hat{A}_{i-1}^n$. First, since $\hat{A}_{i:L}^n$ have already been estimated, from $\hat{A}_i^n$ Receiver 2 obtains the sequence $\hat{\Theta}_i^{(V)} = \hat{A}_i\big[\mathcal{C}_1^{(n)}\big]$ (e.g., yellow squares at Block 3 in Figures 3–6). Given $\hat{\Theta}_i^{(V)}$, it computes $\hat{\tilde{\Theta}}_i^{(V)} = \hat{\Theta}_i^{(V)} \oplus \kappa_\Theta^{(V)}$ (yellow squares with a line through them). Furthermore, Receiver 2 obtains $\hat{\Gamma}_i^{(V)} = \hat{A}_i\big[\mathcal{C}_{1,2}^{(n)}\big]$ (yellow triangles at Block 3 in Figures 3–6). Given this sequence, it computes $\hat{\tilde{\Gamma}}_i^{(V)} = \hat{\Gamma}_i^{(V)} \oplus \kappa_\Gamma^{(V)}$ (yellow triangles with a line through them).

Furthermore, from $\hat{A}_i^n$, Receiver 2 obtains $\hat{\Psi}_{i-1}^{(V)}$ as follows. At block L, in all cases it gets $\hat{\Psi}_{L-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\big]$ directly (all yellow circles at Block L in Figures 3–6). At Block $i \in [2, L-1]$, we distinguish two situations:

- In Case D, Receiver 2 obtains $\hat{\Psi}_{1,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{(n)}\big]$ (e.g., red circles at Block 3 in Figure 6) and $\hat{\Psi}_{2,i-1}^{(V)} \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{\prime(n)}\big]$ (cyan squares with a line through them overlapped by red circles). Since $\hat{\tilde{\Theta}}_{2,i+1}^{(V)}$ (cyan squares with a line through them) has already been estimated, it obtains $\hat{\Psi}_{2,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{\prime(n)}\big] \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)}$ (red circles).
- Otherwise, in other cases, Receiver 2 obtains directly $\hat{\Psi}_{i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{(n)}\big]$ (e.g., red circles at Block 3 in Figures 3–5).

From $\hat{A}_i^n$, Receiver 2 also obtains $\hat{\Gamma}_{i-1}^{(V)}$ as follows. At block L, in all cases it gets $\hat{\tilde{\Gamma}}_{L-1}^{(V)} = \hat{A}_L\big[\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_2^{\prime(n)}\big]$ (e.g., all yellow triangles at Block L in Figures 3–6). At Block $i \in [2, L-1]$, in all cases Receiver 2 obtains $\hat{\Gamma}_{1,i-1}^{(V)} \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big]$ (e.g., red and cyan diamonds with a line through them at Block 3). Since $\hat{\tilde{\Gamma}}_{1,i+1}^{(V)}$ (cyan triangles with a line through them) has already been estimated, Receiver 2 obtains $\hat{\Gamma}_{1,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big] \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)}$ (red triangles). Furthermore, only in Case B, Receiver 2 obtains the sequence $\hat{\Gamma}_{2,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{\prime(n)}\big]$ (remaining red triangles at Block 3 in Figure 4).

Lastly, only in Case A and Case B, Receiver 2 obtains the sequence $\hat{\Pi}_{i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_S^{(n)}\big]$ (e.g., purple crosses at Block 3 in Figure 3 and Figure 4).

Finally, define the sequence $\mathrm{Y}_{(2),i-1}^{\prime(V)} \triangleq \big[\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Pi}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\big]$. Notice that $\mathrm{Y}_{(2),i-1}^{\prime(V)} \supseteq \hat{A}_{i-1}\big[\mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y_{(2)}}^{(n)}\big]$ (elements inside blue curve at Block $i-1$ in Figures 3–6). Thus, Receiver 2 performs SC decoding to form $\hat{A}_{i-1}^n$ by using $\mathrm{Y}_{(2),i-1}^{\prime(V)}$, $\Phi_{(2),i-1}^{(V)}$ and $\tilde{Y}_{(2),i-1}^n$.

5. Performance of the Polar Coding Scheme

The analysis of the polar coding scheme of Section 4 leads to the following theorem.

Theorem 1. *Let $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ be an arbitrary WTBC, such that $\mathcal{X} \in \{0,1\}$. The polar coding scheme described in Section 4 achieves the corner point in Equation (4) of the region $\mathfrak{R}_{\text{CI-WTBC}}$ defined in Proposition 1.*

The proof of Theorem 1 follows in four steps and is provided in the following subsections. In Section 5.1 we show that the polar coding scheme approaches the rate tuple in (4). In Section 5.2 we prove that the joint distribution of $(\tilde{V}_i^n, \tilde{X}_i^n, \tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$, for all $i \in [1, L]$, is asymptotically indistinguishable of the one of the original DMS that is used for the polar code construction. Finally, in Section 5.3 and Section 5.4 we show that the polar coding scheme satisfies the reliability and the secrecy conditions (1) and (2) respectively.

5.1. Transmission Rates

We prove that the polar coding scheme described in Section 4 approaches the rate tuple in Equation (4). Furthermore, we show that the overall length of the secret keys $\kappa_\Theta^{(V)}$, $\kappa_\Gamma^{(V)}$, $\kappa_{\mathrm{Y}\Phi_{(1)}}^{(V)}$ and

$\kappa^{(V)}_{Y\Phi_{(2)}}$, and the additional randomness used in the encoding (besides the randomization sequences) are asymptotically negligible in terms of rate.

5.1.1. Private Message Rate

For $i \in [1, L]$, we have $W_i = \tilde{A}_i\big[\mathcal{C}^{(n)}\big]$. According to the definition of $\mathcal{C}^{(n)}$ in (11), and since $\mathcal{H}^{(n)}_{V|Z} \subseteq \mathcal{H}^{(n)}_{V}$, the rate of $W_{1:L}$ is

$$\frac{1}{nL}\sum_{i=1}^{L}|W_i| = \frac{1}{n}\big|\mathcal{H}^{(n)}_V \cap \big(\mathcal{H}^{(n)}_{V|Z}\big)^{\mathrm{C}}\big| = \frac{1}{n}\big|\mathcal{H}^{(n)}_V\big| - \frac{1}{n}\big|\mathcal{H}^{(n)}_{V|Z}\big| \xrightarrow{n\to\infty} H(V) - H(V|Z)$$

where the limit holds by Lemma 4 of [10]. Therefore, the private message rate achieved by the polar coding scheme is $R_W = I(V;Z)$, as in (4).

5.1.2. Confidential Message Rate

From Section 4.2, in all cases we have $S_1 = \tilde{A}_1\big[\mathcal{I}^{(n)} \cup \mathcal{G}^{(n)}_1 \cup \mathcal{G}^{(n)}_{1,2}\big]$; for $i \in [2, L-1]$, we have $S_i = \tilde{A}_i\big[\mathcal{I}^{(n)}\big]$; and $S_L = \tilde{A}_L\big[\mathcal{I}^{(n)} \cup \mathcal{G}^{(n)}_2\big]$. Thus, we have

$$\begin{aligned}
&\frac{1}{nL}\sum_{i=1}^{L}|S_i| \\
&= \frac{(L-2)}{nL}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{I}^{(n)} \cup \mathcal{G}^{(n)}_1 \cup \mathcal{G}^{(n)}_{1,2}\big| + \big|\mathcal{I}^{(n)} \cup \mathcal{G}^{(n)}_2\big|\Big) \\
&= \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{G}^{(n)}_1\big| + \big|\mathcal{G}^{(n)}_2\big| + \big|\mathcal{G}^{(n)}_{1,2}\big|\Big) \\
&= \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\big|\mathcal{G}^{(n)} \setminus \mathcal{G}^{(n)}_0\big| \\
&\overset{(a)}{=} \frac{1}{n}\Big(\big|\mathcal{G}^{(n)}_0\big| + \big|\mathcal{G}^{(n)}_2\big| - \big|\mathcal{R}^{(n)}_{1,2}\big| - \big|\mathcal{R}'^{(n)}_{1,2}\big| - \big|\mathcal{R}^{(n)}_1\big| - \big|\mathcal{R}'^{(n)}_1\big|\Big) + \frac{1}{nL}\big|\mathcal{G}^{(n)} \setminus \mathcal{G}^{(n)}_0\big| \\
&\overset{(b)}{=} \frac{1}{n}\Big(\big|\mathcal{G}^{(n)}_0\big| + \big|\mathcal{G}^{(n)}_2\big| - \big|\mathcal{C}^{(n)}_1\big| - \big|\mathcal{C}^{(n)}_{1,2}\big|\Big) + \frac{\big|\mathcal{G}^{(n)} \setminus \mathcal{G}^{(n)}_0\big|}{nL} \\
&\overset{(c)}{\geq} \frac{1}{n}\Big(\big|\mathcal{H}^{(n)}_{V|Z} \cap \mathcal{L}^{(n)}_{V|Y_{(1)}}\big| - \big|\big(\mathcal{H}^{(n)}_{V|Z}\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big|\Big) + \frac{1}{nL}\Big|\mathcal{H}^{(n)}_{V|Z} \cap \Big(\mathcal{L}^{(n)}_{V|Y_{(1)}} \cap \mathcal{L}^{(n)}_{V|Y_{(2)}}\Big)^{\mathrm{C}}\Big| \\
&\overset{(d)}{\geq} \frac{1}{n}\Big(\big|\mathcal{H}^{(n)}_{V|Z} \cap \mathcal{L}^{(n)}_{V|Y_{(1)}}\big| - \big|\big(\mathcal{H}^{(n)}_{V|Z}\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big|\Big) + \frac{1}{nL}\Big|\mathcal{H}^{(n)}_{V|Z}\Big| - \frac{1}{nL}\Big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\Big| \\
&= \frac{1}{n}\big|\mathcal{H}^{(n)}_{V|Z}\big| - \frac{1}{n}\big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big| + \frac{1}{nL}\big|\mathcal{H}^{(n)}_{V|Z}\big| - \frac{1}{nL}\big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big| \\
&\xrightarrow{n\to\infty} H(V|Z) - H(V|Y_{(1)}) + \frac{1}{L}\big(H(V|Z) - H(V|Y_{(1)})\big) \\
&\xrightarrow{L\to\infty} H(V|Z) - H(V|Y_{(1)})
\end{aligned}$$

where (a) holds by the definition of $\mathcal{I}^{(n)}$ in (24); (b) holds because, in all cases, we have $\big|\mathcal{R}^{(n)}_{1,2}\big| + \big|\mathcal{R}'^{(n)}_1\big| = \big|\mathcal{C}^{(n)}_{1,2}\big|$ and $\big|\mathcal{R}^{(n)}_1\big| + \big|\mathcal{R}'^{(n)}_{1,2}\big| = \big|\mathcal{C}^{(n)}_1\big|$; (c) follows from the partition of $\mathcal{H}^{(n)}_V$ defined in (12)–(19); (d) follows from applying elementary set operations and because, by assumption, $H(V|Y_{(1)}) \geq H(V|Y_{(2)})$, which means that $\big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big| \geq \big|\big(\mathcal{L}^{(n)}_{V|Y_{(2)}}\big)^{\mathrm{C}}\big|$ (by Lemma 4 of [10]); and the limit when n goes to infinity holds also by Lemma 4 of [10]. Hence, the polar coding scheme operates as close to the rate R_S in (4) as desired by choosing a sufficiently large L.

5.1.3. Randomization Sequence Rate

For $i \in [1, L]$, we have $R_i = \tilde{T}_i\big[\mathcal{H}^{(n)}_{X|V} \cap (\mathcal{H}^{(n)}_{X|VZ})^{\mathrm{C}}\big]$. Since $\mathcal{H}^{(n)}_{X|VZ} \supseteq \mathcal{H}^{(n)}_{X|V}$, we have

$$\frac{1}{nL}\sum_{i=1}^{L}|R_i| = \frac{1}{n}\Big|\mathcal{H}^{(n)}_{X|V} \cap \big(\mathcal{H}^{(n)}_{X|VZ}\big)^{\mathrm{C}}\Big| = \frac{1}{n}\big|\mathcal{H}^{(n)}_{X|V}\big| - \frac{1}{n}\big|\mathcal{H}^{(n)}_{X|VZ}\big| \xrightarrow{n\to\infty} H(X|Z) - H(X|VZ)$$

where the limit holds by Lemma 4 of [10]. Thus, the randomization sequence rate used by the polar coding scheme is $R_R = I(X;Z|V)$ as in (4).

5.1.4. Private-Shared Sequence Rate

Transmitter and legitimate Receiver $k \in [1,2]$ must privately share the keys $\kappa^{(V)}_{\Theta}$, $\kappa^{(V)}_{\Gamma}$ and $\kappa^{(V)}_{\mathrm{Y}\Phi_{(k)}}$. Hence, the overall rate is

$$\begin{aligned}
&\frac{1}{nL}\Big(\big|\kappa^{(V)}_{\Theta}\big| + \big|\kappa^{(V)}_{\Gamma}\big| + \sum_{k=1}^{2}\big|\kappa^{(V)}_{\mathrm{Y}\Phi_{(k)}}\big|\Big)\\
&\quad= \frac{1}{nL}\Big(\big|\mathcal{C}^{(n)}_{1}\big| + \big|\mathcal{C}^{(n)}_{1,2}\big|\Big) + \frac{1}{nL}\sum_{k=1}^{2}\Big(L\big|(\mathcal{H}^{(n)}_{V})^{\mathrm{C}} \cap (\mathcal{L}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}\big| + \big|\mathcal{H}^{(n)}_{V} \cap (\mathcal{L}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}\big|\Big)\\
&\quad\overset{(a)}{=} \frac{1}{nL}\Big(\big|\mathcal{H}^{(n)}_{V} \cap (\mathcal{H}^{(n)}_{V|Z})^{\mathrm{C}} \cap (\mathcal{L}^{(n)}_{V|Y_{(1)}})^{\mathrm{C}}\big|\Big)\\
&\qquad+ \frac{1}{nL}\sum_{k=1}^{2}\Big(L\big|(\mathcal{H}^{(n)}_{V})^{\mathrm{C}} \cap (\mathcal{L}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}\big| + \big|\mathcal{H}^{(n)}_{V} \cap (\mathcal{L}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}\big|\Big)\\
&\quad\overset{(b)}{\leq} \frac{1}{nL}\big|(\mathcal{L}^{(n)}_{V|Y_{(1)}})^{\mathrm{C}}\big| + \frac{1}{nL}\sum_{k=1}^{2}\Big(L\big|(\mathcal{H}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}} \cap (\mathcal{L}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}\big| + \big|(\mathcal{L}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}\big|\Big)\\
&\quad\xrightarrow{n\to\infty} \frac{1}{L}\big(2H(V|Y_{(1)}) + H(V|Y_{(2)})\big)\\
&\quad\xrightarrow{L\to\infty} 0,
\end{aligned}$$

where (a) follows from the definition of $\mathcal{C}^{(n)}_{1}$ and $\mathcal{C}^{(n)}_{1,2}$ in (17) and (19), respectively; (b) follows from standard set properties and because $(\mathcal{H}^{(n)}_{V|Z})^{\mathrm{C}} \subseteq (\mathcal{H}^{(n)}_{V|Y_{(k)}})^{\mathrm{C}}$ for any $k \in [1,2]$; and the limit when n goes to infinity holds by Lemma 4 of [10].

5.1.5. Rate of the Additional Randomness

Besides the randomization sequences $R_{1:L}$, the encoder uses the random sequence $\Lambda^{(X)}_{0}$, with size $\big|\mathcal{H}^{(n)}_{X|V}\big|$, for the polar-based channel prefixing. Moreover, for $i \in [1, L]$, the encoder randomly draws those elements $\tilde{A}_i(j)$ such that $j \in (\mathcal{H}^{(n)}_{V})^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V}$, and those elements $\tilde{T}_i(j)$ such that $j \in (\mathcal{H}^{(n)}_{X|V})^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{X|V}$. Nevertheless, we have

$$\begin{aligned}
&\frac{1}{nL}\Big(\big|\mathcal{H}^{(n)}_{X|V}\big| + L\big|(\mathcal{H}^{(n)}_{V})^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V}\big| + L\big|(\mathcal{H}^{(n)}_{X|V})^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{X|V}\big|\Big)\\
&\quad\xrightarrow{n\to\infty} \frac{1}{L}H(X|V)\\
&\quad\xrightarrow{L\to\infty} 0,
\end{aligned}$$

where the limit when n approaches to infinity follows from applying Lemma 4 of [10].

5.2. Distribution of the DMS after the Polar Encoding

For $i \in [1, L]$, let $\tilde{q}_{A_i^n T_i^n}$ denote the distribution of $(\tilde{A}_i^n, \tilde{T}_i^n)$ after the encoding. The following lemma proves that $\tilde{q}_{A_i^n T_i^n}$ and the marginal distribution $p_{A^n T^n}$ of the original DMS are nearly statistically indistinguishable for sufficiently large n and, consequently, so are $\tilde{q}_{V_i^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}$ and $p_{V^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}$. This result is crucial for the reliability and secrecy performance of the polar coding scheme.

Lemma 1. *For any $i \in [1, L]$, we obtain*

$$\mathbb{V}(\tilde{q}_{A_i^n T_i^n}, p_{A^n T^n}) \leq \delta_n^{(*)},$$
$$\mathbb{V}(\tilde{q}_{V_i^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}, p_{V^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}) \leq \delta_n^{(*)},$$

where $\delta_n^{(*)} \triangleq 2n\sqrt{4\sqrt{n\delta_n \ln 2}\big(2n - \log\big(2\sqrt{n\delta_n \ln 2}\big)\big) + \delta_n} + 2\sqrt{n\delta_n \ln 2}$.

Proof. Omitted because it follows similar reasoning as in Lemma 3 of [11]. □

5.3. Reliability Analysis

In this section we prove that both legitimate receivers can reliably reconstruct the private and the confidential messages $(W_{1:L}, S_{1:L})$ with arbitrary small error probability.

For $i \in [1, L]$ and $k \in [1, 2]$, let $\tilde{q}_{V_i^n Y_{(k),i}^n}$ and $p_{V^n Y_{(k)}^n}$ be marginals of $\tilde{q}_{V_i^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}$ and $p_{V^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}$ respectively, and define an optimal coupling Proposition 4.7 of [25] between $\tilde{q}_{V_i^n Y_{(k),i}^n}$ and $p_{V^n Y_{(k)}^n}$ such that $\mathbb{P}\big[\mathcal{E}_{V_i^n Y_{(k),i}^n}\big] = \mathbb{V}\big(\tilde{q}_{V_i^n Y_{(k),i}^n}, p_{V^n Y_{(k)}^n}\big)$, where $\mathcal{E}_{V_i^n Y_{(k),i}^n} \triangleq \big\{\big(\tilde{V}_i^n, \tilde{Y}_{(k),i}^n\big) \neq \big(V^n, Y_{(k)}^n\big)\big\}$. Additionally, define the error event

$$\mathcal{E}_{(k),i} \triangleq \Big\{\hat{A}_i\big[\big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big] \neq \tilde{A}_i\big[\big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big]\Big\}.$$

Recall that $(\mathrm{Y}_{(k)}^{(V)}, \Phi_{(k),1:L}^{(V)})$ is available to Receiver $k \in [1, 2]$. Thus, $\mathbb{P}[\mathcal{E}_{(1),1}] = \mathbb{P}[\mathcal{E}_{(2),L}] = 0$ because given $\mathrm{Y}_{(1)}^{(V)}$ and $\Phi_{(1),1}^{(V)}$ legitimate Receiver 1 knows $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$, and given $\mathrm{Y}_{(2)}^{(V)}$ and $\Phi_{(2),L}^{(V)}$ legitimate Receiver 2 knows $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$. Moreover, due to the chaining structure, in Section 4.4 we have seen that $\tilde{A}_i\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ is repeated in $\tilde{A}_{i-1}^n$ for $i \in [2, L]$. Therefore, at legitimate Receiver 1, for $i \in [2, L]$ we have

$$\mathbb{P}[\mathcal{E}_{(1),i}] \leq \mathbb{P}\big[\hat{A}_{i-1}^n \neq \tilde{A}_{i-1}^n\big]. \tag{35}$$

Similarly, due to the chaining construction, we have seen that $\tilde{A}_i\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ is repeated in $\tilde{A}_{i+1}^n$ for $i \in [1, L-1]$. Thus, at legitimate Receiver 2, for $i \in [1, L-1]$ we obtain

$$\mathbb{P}[\mathcal{E}_{(2),i}] \leq \mathbb{P}\big[\hat{A}_{i+1}^n \neq \tilde{A}_{i+1}^n\big]. \tag{36}$$

Hence, the probability of incorrectly decoding (W_i, S_i) at the Receiver $k \in [1,2]$ is

$$\begin{aligned}
\mathbb{P}\big[(W_i, S_i) \neq (\hat{W}_i, \hat{S}_i)\big] &\leq \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n\big] \\
&= \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n \big| \mathcal{E}^{\mathsf{C}}_{V_i^n Y^n_{(k),i}} \cap \mathcal{E}^{\mathsf{C}}_{(k),i}\big] \mathbb{P}\big[\mathcal{E}^{\mathsf{C}}_{V_i^n Y^n_{(k),i}} \cap \mathcal{E}^{\mathsf{C}}_{(k),i}\big] \\
&\quad + \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n \big| \mathcal{E}_{V_i^n Y^n_{(k),i}} \cup \mathcal{E}_{(k),i}\big] \mathbb{P}\big[\mathcal{E}_{V_i^n Y^n_{(k),i}} \cup \mathcal{E}_{(k),i}\big] \\
&\leq \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n \big| \mathcal{E}^{\mathsf{C}}_{V_i^n Y^n_{(k),i}} \cap \mathcal{E}^{\mathsf{C}}_{(k),i}\big] + \mathbb{P}\big[\mathcal{E}_{V_i^n Y^n_{(k),i}}\big] + \mathbb{P}\big[\mathcal{E}_{(k),i}\big] \\
&\overset{(a)}{\leq} n\delta_n + \mathbb{P}\big[\mathcal{E}_{V_i^n Y^n_{(k),i}}\big] + \mathbb{P}\big[\mathcal{E}_{(k),i}\big] \\
&\overset{(b)}{\leq} n\delta_n + \delta_n^{(*)} + \mathbb{P}\big[\mathcal{E}_{(k),i}\big] \\
&\overset{(c)}{\leq} i\big(n\delta_n + \delta_n^{(*)}\big),
\end{aligned}$$

where (a) holds by Th. 2 of [19]; (b) follows from the optimal coupling and Lemma 1; and (c) holds by induction and Equations (35) and (36). Therefore, by the union bound we obtain

$$\mathbb{P}\big[(W_{1:L}, S_{1:L}) \neq (\hat{W}_{1:L}, \hat{S}_{1:L})\big] \leq \sum_{i=1}^{L} \mathbb{P}\big[\tilde{A}_i^n \neq \hat{A}_i^n\big] \leq \frac{L(L+1)}{2}\big(n\delta_n + 2\delta_n^{(*)}\big),$$

and for sufficiently large n the polar coding scheme satisfies the reliability condition in (1).

5.4. Secrecy Analysis

Since encoding in Section 4 takes place over L blocks of size n, we need to prove that

$$\lim_{n\to\infty} I(S_{1:L}, \tilde{Z}_{1:L}^n) = 0.$$

For clarity and with slight abuse of notation, for any Block $i \in [1, L]$ let

$$\Xi_i^{(V)} \triangleq \big[\Pi_i^{(V)}, \Lambda_i^{(V)}, \Psi_i^{(V)}, \Gamma_i^{(V)}\big],$$

which denotes the entire sequence depending on $\tilde{A}_i^n$ that is repeated at Block $i+1$. Furthermore, let

$$\bar{\Omega}_i^{(V)} \triangleq [\bar{\Theta}_i^{(V)}, \bar{\Gamma}_i^{(V)}],$$

which represents the sequence depending on $\tilde{A}_i^n$ that is repeated at Block $i-1$. Furthermore, we define $\kappa_\Omega^{(V)} \triangleq [\kappa_\Theta^{(V)}, \kappa_\Gamma^{(V)}]$. Then, a Bayesian graph describing the dependencies between all the variables involved in the polar coding scheme of Section 4 is given in Figure 7.

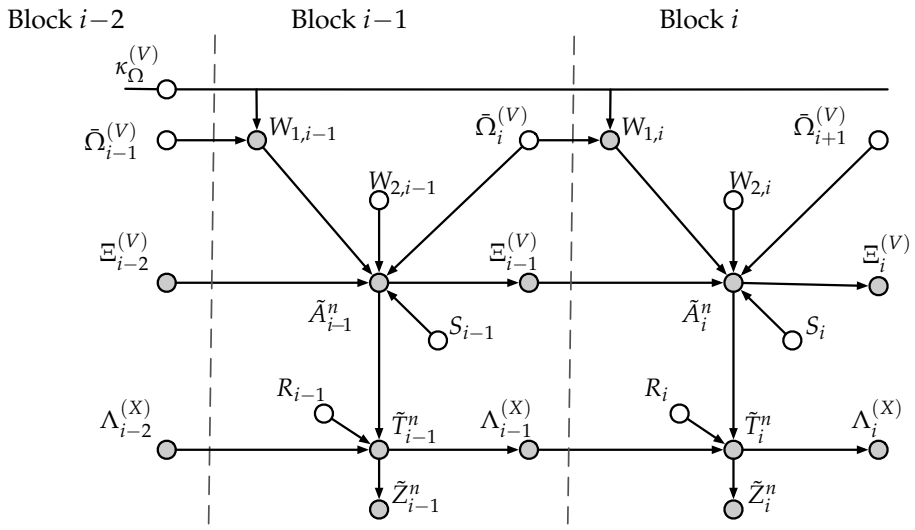

Figure 7. Graphical representation (Bayesian graph) of the dependencies between random variables involved in the polar coding scheme. Independent random variables are indicated by white nodes, whereas those that are dependent are indicated by gray nodes.

Despite $\Gamma_i^{(V)} \subseteq \Xi_i^{(V)}$ and $\bar{\Gamma}_i^{(V)} = \Gamma_i^{(V)} \oplus \kappa_\Gamma^{(V)} \subseteq \bar{\Omega}_i^{(V)}$, we represent $\Xi_i^{(V)}$ and $\bar{\Omega}_i^{(V)}$ as two separate nodes in the Bayesian graph because, by *crypto lemma* [26], $\Gamma_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are statistically independent. Furthermore, for convenience, we have considered that dependencies only take place forward (from Block i to Block $i+1$), which is possible by reformulating the encoding as follows. According to Section 4.1, for any $i \in [1, L]$ we have $\tilde{A}_i[\mathcal{C}^{(n)}] = W_i$. Consequently, we can write $W_i \triangleq [W_{1,i}, W_{2,i}]$, where $W_{1,i} \triangleq \tilde{A}_i[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ and $W_{2,i} \triangleq \tilde{A}_i[\mathcal{C}_2^{(n)} \cup \mathcal{C}_0^{(n)}]$. Since $\bar{\Theta}_i^{(V)} = \tilde{A}_i[\mathcal{C}_1^{(n)}] \oplus \kappa_\Theta^{(V)}$ and $\bar{\Gamma}_i^{(V)} = \tilde{A}_i[\mathcal{C}_{1,2}^{(n)}] \oplus \kappa_\Gamma^{(V)}$, we regard $\bar{\Omega}_i^{(V)}$ as an independent random sequence generated at Block $i-1$ that is stored properly into some part of $\tilde{A}_{i-1}[\mathcal{G}^{(n)}]$. Then, we consider that the encoder obtains $W_{1,i} \triangleq \bar{\Omega}_i^{(V)} \oplus \kappa_\Omega^{(V)}$, which is stored into $\tilde{A}_i[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ at Block i. On the other hand, the remaining part $W_{2,i}$ is independently generated at Block i. Recall that the *secret-key* $\kappa_\Omega^{(V)}$ is reused in all blocks.

The following lemma shows that strong secrecy holds for any Block $i \in [1, L]$.

Lemma 2. *For any $i \in [1, L]$ and sufficiently large n,*

$$I\big(S_i \Xi_{i-1}^{(V)} \Lambda_{i-1}^{(X)}; \tilde{Z}_i^n\big) \leq \delta_n^{(\mathrm{S})},$$

where $\delta_n^{(\mathrm{S})} \triangleq 2n\delta_n + 2\delta_n^{(*)}\big(2n - \log \delta_n^{(*)}\big)$ and $\delta_n^{(*)}$ defined as in Lemma 1.

Proof. For n sufficiently large, we have

$$\begin{aligned}
&I\big(S_i \Xi_{i-1}^{(V)} \Lambda_{i-1}^{(X)}; \tilde{Z}_i^n\big) \\
&\quad \overset{(a)}{=} I\big(\tilde{A}_i[\mathcal{H}_{V|Z}^{(n)}] \tilde{T}_i[\mathcal{H}_{X|VZ}^{(n)}]; \tilde{Z}_i^n\big) \\
&\quad \overset{(b)}{=} \big|\mathcal{H}_{V|Z}^{(n)}\big| + \big|\mathcal{H}_{X|VZ}^{(n)}\big| - H\big(\tilde{A}_i[\mathcal{H}_{V|Z}^{(n)}] \tilde{T}_i[\mathcal{H}_{X|VZ}^{(n)}] \big| \tilde{Z}_i^n\big) \\
&\quad \overset{(c)}{\leq} \big|\mathcal{H}_{V|Z}^{(n)}\big| + \big|\mathcal{H}_{X|VZ}^{(n)}\big| - H\big(A[\mathcal{H}_{V|Z}^{(n)}] T[\mathcal{H}_{X|VZ}^{(n)}] \big| Z_i^n\big) + 4n\delta_n^{(*)} - 2\delta_n^{(*)} \log \delta_n^{(*)} \\
&\quad \overset{(d)}{\leq} 2n\delta_n + 4n\delta_n^{(*)} - 2\delta_n^{(*)} \log \delta_n^{(*)}
\end{aligned}$$

where (a) holds by the encoding described in Section 4; (b) holds by the uniformity of $\tilde{A}_i\big[\mathcal{H}_{V|Z}^{(n)}\big]$ and $\tilde{A}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]$; (c) holds because, for n large enough, we obtain

$$\begin{aligned}
&\Big|H\big(\tilde{A}_i\big[\mathcal{H}_{V|Z}^{(n)}\big]\tilde{T}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|\tilde{Z}_i^n\big) - H\big(A_i\big[\mathcal{H}_{V|Z}^{(n)}\big]T_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|Z_i^n\big)\Big| \\
&\quad\le \big|H\big(\tilde{Z}_m^n\big) - H\big(Z_m^n\big)\big| + \Big|H\big(\tilde{A}_i\big[\mathcal{H}_{V|Z}^{(n)}\big]\tilde{T}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]\tilde{Z}_i^n\big) - H\big(A_i\big[\mathcal{H}_{V|Z}^{(n)}\big]T_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]Z_i^n\big)\Big| \\
&\quad\le \mathbb{V}\big(\tilde{q}_{Z_m^n}, p_{Z_m^n}\big)\log\frac{2^n}{\mathbb{V}\big(\tilde{q}_{Z_m^n}, p_{Z_m^n}\big)} \\
&\qquad + \mathbb{V}\big(\tilde{q}_{A_i[\mathcal{H}_{V|Z}^{(n)}]T_i[\mathcal{H}_{X|VZ}^{(n)}]Z^n}, p_{A_i[\mathcal{H}_{V|Z}^{(n)}]T_i[\mathcal{H}_{X|VZ}^{(n)}]Z^n}\big)\log\frac{2^{\left(n+|\mathcal{H}_{V|Z}^{(n)}|+|\mathcal{H}_{X|VZ}^{(n)}|\right)}}{\mathbb{V}\big(\tilde{q}_{A_i[\mathcal{H}_{V|Z}^{(n)}]T_i[\mathcal{H}_{X|VZ}^{(n)}]Z^n}, p_{A_i[\mathcal{H}_{V|Z}^{(n)}]T_i[\mathcal{H}_{X|VZ}^{(n)}]Z^n}\big)} \\
&\quad\overset{(b)}{\le} 4n\delta_{\text{ld-nls}}^{(n)} - 2\delta_{\text{ld-nls}}^{(n)}\log\delta_{\text{ld-nls}}^{(n)},
\end{aligned}$$

where we have used the chain rule of entropy and the triangle inequality, [27, Lemma 30], the fact that the function $x \to x\log x$ is decreasing for $x > 0$ small enough and Lemma 1; and, lastly, (d) holds because

$$\begin{aligned}
&H\big(A\big[\mathcal{H}_{V|Z}^{(n)}\big]T\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|Z^n\big) \\
&\quad\ge H\big(A\big[\mathcal{H}_{V|Z}^{(n)}\big]\big|Z^n\big) + H\big(T\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|A^nZ^n\big) \\
&\quad\ge \sum_{j\in\mathcal{H}_{V|Z}^{(n)}} H\big(A(j)\big|A^{1:j-1}Z^n\big) + \sum_{j\in\mathcal{H}_{X|VZ}^{(n)}} H\big(T(j)\big|T^{1:j-1}V^nZ^n\big) \\
&\quad\ge \big|\mathcal{H}_{V|Z}^{(n)}\big|(1-\delta_n) + \big|\mathcal{H}_{X|VZ}^{(n)}\big|(1-\delta_n)
\end{aligned}$$

where we have used the fact that conditioning does not increase entropy, the invertibility of G_n, and the definition of $\mathcal{H}_{V|Z}^{(n)}$ and $\mathcal{H}_{X|VZ}^{(n)}$ in (6) and (9) respectively. □

Next, the following lemma shows that eavesdropper observations $\tilde{Z}_i^n$ are asymptotically statistically independent of observations $\tilde{Z}_{1:i-1}^n$ from previous blocks.

Lemma 3. *For any $i \in [2, L]$ and sufficiently large n,*

$$I\big(S_{1:L}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n\big) \le \delta_n^{(\mathrm{S})},$$

where $\delta_n^{(\mathrm{S})}$ is defined as in Lemma 2.

Proof. For any $i \in [2, L]$ and sufficiently large n, we have

$$
\begin{aligned}
& I\big(S_{1:L}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i\big) \\
&\quad = I\big(S_{1:i}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i\big) + I\big(S_{i+1:L}; \tilde{Z}^n_i \big| S_{1:i}\tilde{Z}^n_{1:i-1}\big) \\
&\quad \overset{(a)}{=} I\big(S_{1:i}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i\big) \\
&\quad \leq I\big(S_{1:i}\tilde{Z}^n_{1:i-1}\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}; \tilde{Z}^n_i\big) \\
&\quad = I\big(S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}; \tilde{Z}^n_i\big) + I\big(S_{1:i-1}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad \overset{(b)}{\leq} \delta^{(\mathrm{S})}_n + I\big(S_{1:i-1}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad \leq \delta^{(\mathrm{S})}_n + I\big(S_{1:i-1}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i W_{1,i} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad = \delta^{(\mathrm{S})}_n + I\big(S_{1:i-1}\tilde{Z}^n_{1:i-1}; W_{1,i} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) + I\big(S_{1:i-1}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}W_{1,i}\big) \\
&\quad \overset{(c)}{=} \delta^{(\mathrm{S})}_n + I\big(S_{1:i-1}\tilde{Z}^n_{1:i-1}; W_{1,i} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad \leq \delta^{(\mathrm{S})}_n + I\big(\tilde{A}^n_{1:i-1}\tilde{Z}^n_{1:i-1}; W_{1,i} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad = \delta^{(\mathrm{S})}_n + I\big(\tilde{A}^n_{1:i-1}; W_{1,i} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) + I\big(\tilde{Z}^n_{1:i-1}; W_{1,i} \big| \tilde{A}^n_{1:i-1}S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad \overset{(d)}{=} \delta^{(\mathrm{S})}_n + I\big(\tilde{A}^n_{1:i-1}; W_{1,i} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad \overset{(e)}{=} \delta^{(\mathrm{S})}_n + I\big(\tilde{A}^n_{1:i-1}; \bar{\Omega}^{(V)}_i \oplus \kappa^{(V)}_{\Omega} \big| S_i\Xi^{(V)}_{i-1}\Lambda^{(X)}_{i-1}\big) \\
&\quad \overset{(f)}{=} \delta^{(\mathrm{S})}_n
\end{aligned}
$$

where (a) holds by independence between $S_{i+1:L}$ and any random variable from Blocks 1 to i; (b) holds by Lemma 2; (c) follows from applying d-separation [28] over the Bayesian graph in Figure 7 to obtain that $\tilde{Z}^n_i$ and $(S_{1:i-1}, \tilde{Z}^n_{1:i-1})$ are conditionally independent given $(S_i, \Xi^{(V)}_{i-1}, \Lambda^{(X)}_{i-1}, W_{1,i})$; (d) also follows from applying *d-separation* to obtain that $W_{1,i}$ and $\tilde{Z}^n_{1:i-1}$ are conditionally independent given $(\tilde{A}^n_{1:i-1}, S_i, \Xi^{(V)}_{i-1}, \Lambda^{(X)}_{i-1})$; (e) holds by definition; and (f) holds because $\bar{\Omega}^{(V)}_i$ is independent of $(S_i, \Xi^{(V)}_{i-1}, \Lambda^{(X)}_{i-1})$ and any random variable from Block 1 to $(i-2)$, and because from applying crypto-lemma [26] we obtain that $\bar{\Omega}^{(V)}_i \oplus \kappa^{(V)}_{\Omega}$ is independent of $\tilde{A}^n_{i-1}$. □

Therefore, we obtain

$$
\begin{aligned}
I\big(S_{1:L}; \tilde{Z}^n_{1:L}\big) &\overset{(a)}{=} I\big(S_{1:L}; \tilde{Z}^n_1\big) + \sum_{i=2}^{L} I\big(S_{1:L}; \tilde{Z}^n_i \big| \tilde{Z}^n_{1:i-1}\big) \\
&\overset{(b)}{\leq} I\big(S_{1:L}; \tilde{Z}^n_1\big) + (L-1)\delta^{(\mathrm{S})}_n \\
&= I\big(S_1; \tilde{Z}^n_1\big) + I\big(S_{2:L}; \tilde{Z}^n_1 \big| S_1\big) + (L-1)\delta^{(\mathrm{S})}_n \\
&\overset{(c)}{=} I\big(S_1; \tilde{Z}^n_1\big) + (L-1)\delta^{(\mathrm{S})}_n \\
&\overset{(d)}{\leq} L\delta^{(\mathrm{S})}_n
\end{aligned}
$$

where (a) follows from applying the chain rule; (b) holds by Lemma 3; (c) holds by independence between $S_{2:L}$ and any random variable from Block 1; and (d) holds by Lemma 2. Thus, for sufficiently large n the polar coding scheme satisfies the strong secrecy condition in (2).

Remark 1. *We conjecture that the use $\kappa^{(V)}_{\Omega}$ is not needed for the polar coding scheme to satisfy the strong secrecy condition. However, the key is required in order to prove this condition by means of analyzing a causal Bayesian graph similar to the one in Figure 7.*

Remark 2. *Although backward dependencies between random variables of different blocks appear in [12], a secret seed as* $\kappa_{\Omega}^{(V)}$ *is not necessary for the polar coding scheme to provide strong secrecy. This is because random sequences that are repeated in adjacent blocks are stored only into those corresponding entries whose indices belong to the "high entropy set given eavesdropper observations", i.e., the equivalent sets of* $\mathcal{H}_{V|Z}^{(n)}$ *and* $\mathcal{H}_{X|VZ}^{(n)}$ *in our polar coding scheme. By contrast, notice that our polar coding scheme repeats* $\left[\Theta_i^{(V)}, \Gamma_i^{(V)}\right] \subseteq \tilde{A}_i\left[(\mathcal{H}_{V|Z}^{(n)})^{\mathrm{C}}\right]$.

Remark 3. *Another possibility for the polar coding scheme is to repeat at Block* $i+1$ *the modulo-2 addition between* $\left[\Psi_i^{(V)}, \Gamma_i^{(V)}\right]$ *and a particular secret-key, instead of repeating an* encrypted *version of* $\left[\Theta_i^{(V)}, \Gamma_i^{(V)}\right]$ *at Block* $i-1$. *Then, it is not difficult to prove that* $I\left(S_{1:L}\tilde{Z}_{i+1:L}^{n}; \tilde{Z}_i^n\right) \leq \delta_n^{(\mathrm{S})}$ *(similar to Lemma 3). Thus, one can minimize the length of this secret-key depending on whether* $\left|\mathcal{C}_1^{(n)}\right| < \left|\mathcal{C}_2^{(n)}\right|$ *or vice versa.*

6. Concluding Remarks

A strongly secure polar coding scheme is proposed for the WTBC with two legitimate receivers and one eavesdropper. This polar code achieves the best known inner-bound on the achievable region of the CI-WTBC model, where a transmitter wants to send common information (private and confidential) to both receivers. Due to the non-degradedness assumption of the channel, the encoder builds a chaining construction that induces bidirectional dependencies between adjacent blocks, which need to be taken carefully into account in the secrecy analysis.

These bidirectional dependencies involve elements from adjacent blocks whose indices belong to the "low entropy sets given eavesdropper observations". Consequently, in order to prove that the polar coding scheme satisfies the strong secrecy condition, we have introduced a secret-key whose length becomes negligible in terms of rate as the number of blocks grows indefinitely. In the proposed polar coding scheme, this key has been used to randomize part of these elements from any block that are repeated in the previous (or next) one. In this way, we can analyze the dependencies between all random variables involved in the secrecy analysis by means of a causal Bayesian graph and apply d-separation to prove that the polar coding scheme induces eavesdropper's observations that are statistically independent of one another.

Despite the good performance of the polar coding schemes, some issues still persist. First, it is worth saying that the additional secret transmission (that is negligible in terms of rate) required to initialize the decoding algorithms at both receivers can be omitted by using a similar approach as in [29], where an initialization phase to generate a secret-key can be performed without worsening the communication rate. On the other hand, how to replace the random decisions entirely by deterministic ones in SC encoding is a problem that still remains unsolved. Additionally, we conjecture that the previous secret-keys that are used to prove independence between blocks are not necessary. However, how to prove this independence without using them seems a difficult problem to address at this point.

Acknowledgments: This work has been funded by the AEI of Ministerio de Ciencia, Innovación y Universidades of Spain, TEC2016-75067-C4-2-R and RED2018-102668-T with ESF and Dept. d'Empresa i Coneixement de la Generalitat de Catalunya, 2017 SGR 578 AGAUR and 001-P-001644 QuantumCAT with ERDF.

Author Contributions: Conceptualization, J.d.O.A. and J.R.F.; formal analysis, J.d.O.A.; funding acquisition, J.R.F.; investigation, J.d.O.A. and J.R.F.; methodology, J.d.O.A. and J.R.F; supervision, J.R.F.; validation, J.R.F.; writing–original draft, J.d.O.A.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

WTBC	Wiretap broadcast channel
CI-WTBC	Common information over the wiretap broadcast channel
SC	Successive cancellation
DMS	Discrete memoryless source

References

1. Wyner, A. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387; doi:10.1002/j.1538-7305.1975.tb02040.x.
2. Csiszár, I.; Korner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348; doi:10.1109/TIT.1978.1055892.
3. Maurer, U.; Wolf, S. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology—EUROCRYPT 2000*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 351–368.
4. Arikan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 3051–3073.
5. Mahdavifar, H.; Vardy, A. Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes. *IEEE Trans. Inf. Theory* **2011**, *57*, 6428–6443; doi:10.1109/TIT.2011.2162275.
6. Sasoglu, E.; Vardy, A. A new polar coding scheme for strong security on wiretap channels. In Proceedings of 2013 IEEE International Symposium on Information Theory (ISIT), Istanbul, Turkey, 7–12 July 2013; pp. 1117–1121; doi:10.1109/ISIT.2013.6620400.
7. Renes, J.M.; Renner, R.; Sutter, D. Efficient one-way secret-key agreement and private channel coding via polarization. In *Advances in Cryptology-ASIACRYPT*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 194–213.
8. Wei, Y.; Ulukus, S. Polar Coding for the General Wiretap Channel With Extensions to Multiuser Scenarios. *IEEE J. Sel. Areas Commun.* **2016**, *34*, 278–291; doi:10.1109/JSAC.2015.2504275.
9. Gulcu, T.C.; Barg, A. Achieving Secrecy Capacity of the Wiretap Channel and Broadcast Channel With a Confidential Component. *IEEE Trans. Inf. Theory* **2017**, *63*, 1311–1324; doi:10.1109/TIT.2016.2631223.
10. Chou, R.A.; Bloch, M.R. Polar Coding for the Broadcast Channel With Confidential Messages: A Random Binning Analogy. *IEEE Trans. Inf. Theory* **2016**, *62*, 2410–2429; doi:10.1109/TIT.2016.2539145.
11. del Olmo Alos, J.; Rodríguez Fonollosa, J. Strong Secrecy on a Class of Degraded Broadcast Channels Using Polar Codes. *Entropy* **2018**, *20*, 467; doi:10.3390/e20060467.
12. Chou, R.A.; Yener, A. Polar Coding for the Multiple Access Wiretap Channel via Rate-Splitting and Cooperative Jamming. *IEEE Trans. Inf. Theory* **2018**, *64*, 7903–7921; doi:10.1109/TIT.2018.2865741.
13. Chia, Y.K.; El Gamal, A. Three-receiver broadcast channels with common and confidential messages. *IEEE Trans. Inf. Theory* **2012**, *58*, 2748–2765.
14. Hassani, S.; Urbanke, R. Universal polar codes. In Proceedings of 2014 IEEE International Symposium on Information Theory (ISIT), Honolulu, HI, USA, 29 June–4 July 2014; pp. 1451–1455.
15. Mondelli, M.; Hassani, S.; Sason, I.; Urbanke, R. Achieving Marton's region for broadcast channels using polar codes. *IEEE Trans. Inf. Theory* **2015**, *61*, 783–800; doi:10.1109/TIT.2014.2368555.
16. Watanabe, S.; Oohama, Y. The optimal use of rate-limited randomness in broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **2015**, *61*, 983–995.
17. Karzand, M.; Telatar, E. Polar codes for q-ary source coding. In Proceedings of 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 909–912; doi:10.1109/ISIT.2010.5513555.
18. Şasoğlu, E.; Telatar, E.; Arikan, E. Polarization for arbitrary discrete memoryless channels. In Proceedings of 2009 IEEE Information Theory Workshop, Taormina, Italy, 11–16 October 2009; pp. 144–148.
19. Arikan, E. Source polarization. In Proceedings of 2010 IEEE International Symposium on Information Theory, Austin, TX, USA, 13–18 June 2010; pp. 899–903.
20. Tal, I.; Vardy, A. How to construct polar codes. *IEEE Trans. Inf. Theory* **2013**, *59*, 6562–6582.
21. Vangala, H.; Viterbo, E.; Hong, Y. A comparative study of polar code constructions for the AWGN channel. *arXiv* **2015**, arXiv:1501.02473 .
22. Honda, J.; Yamamoto, H. Polar Coding Without Alphabet Extension for Asymmetric Models. *IEEE Trans. Inf. Theory* **2013**, *59*, 7829–7838; doi:10.1109/TIT.2013.2282305.
23. Korada, S.B.; Urbanke, R.L. Polar codes are optimal for lossy source coding. *IEEE Trans. Inf. Theory* **2010**, *56*, 1751–1768.
24. Chou, R.A.; Bloch, M.R. Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes. In Proceedings of 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 29 September–2 October 2015; pp. 1380–1385; doi:10.1109/ALLERTON.2015.7447169.

25. Levin, D.A.; Peres, Y.; Wilmer, E.L. *Markov Chains and Mixing Times*; American Mathematical Society: Providence, RI, USA, 2009.
26. Forney, G.D., Jr. On the role of MMSE estimation in approaching the information-theoretic limits of linear Gaussian channels: Shannon meets Wiener. In Proceedings of the 41st Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 1–3 October, 2003.
27. Csiszar, I.; Körner, J. *Information Theory: Coding Theorems for Discrete Memoryless Systems*; Cambridge University Press: Cambridge, UK, 2011.
28. Pearl, J. *Causality*; Cambridge University Press: Cambridge, UK, 2009.
29. Chou, R.A. Explicit Codes for the Wiretap Channel with Uncertainty on the Eavesdropper's Channel. In Proceedings of 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 476–480; doi:10.1109/ISIT.2018.8437777.